



# Troubleshooting ExpressWay & Mobile Remote Access

Michael Huang

Customer Support Engineer - China TAC Collaboration

# Agenda

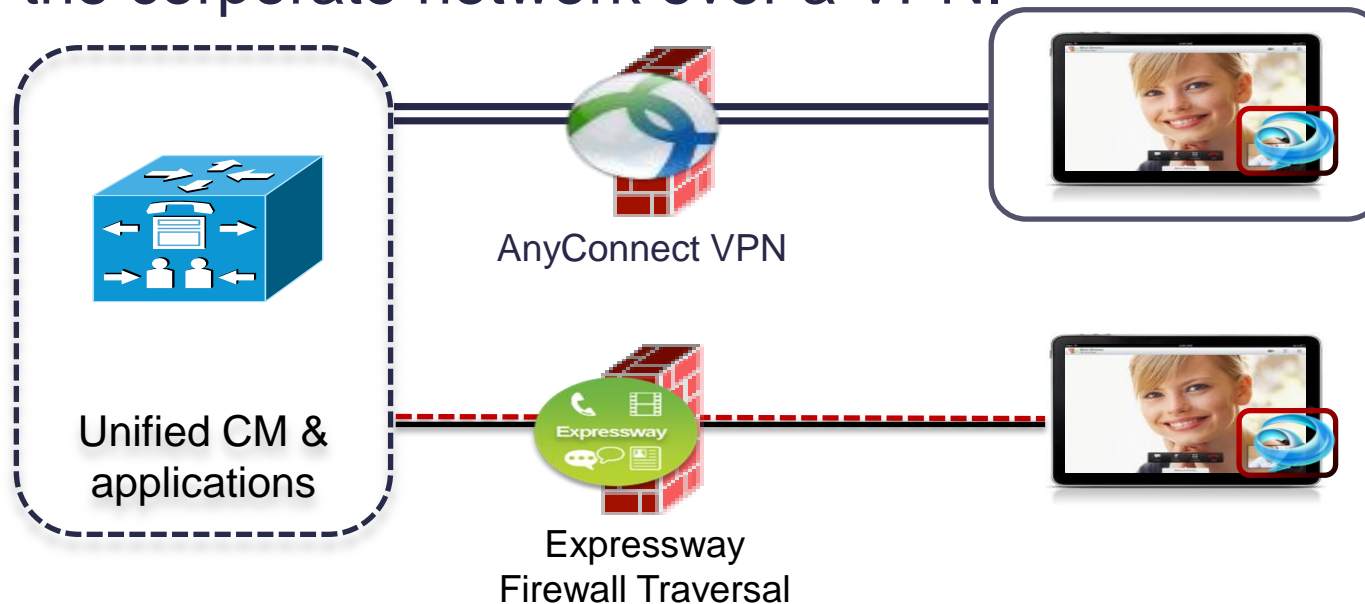
- Overview, ExpressWay and Mobile Remote Access
- ExpressWay Configuration
  - Firewall Settings
  - Certificate Requirements
  - Traversal Zone setup
  - UC server discovery
  - Domain and DNS
- ExpressWay serviceability
- Jabber registration and call walk through

# What is 'Mobile and Remote Access' feature?

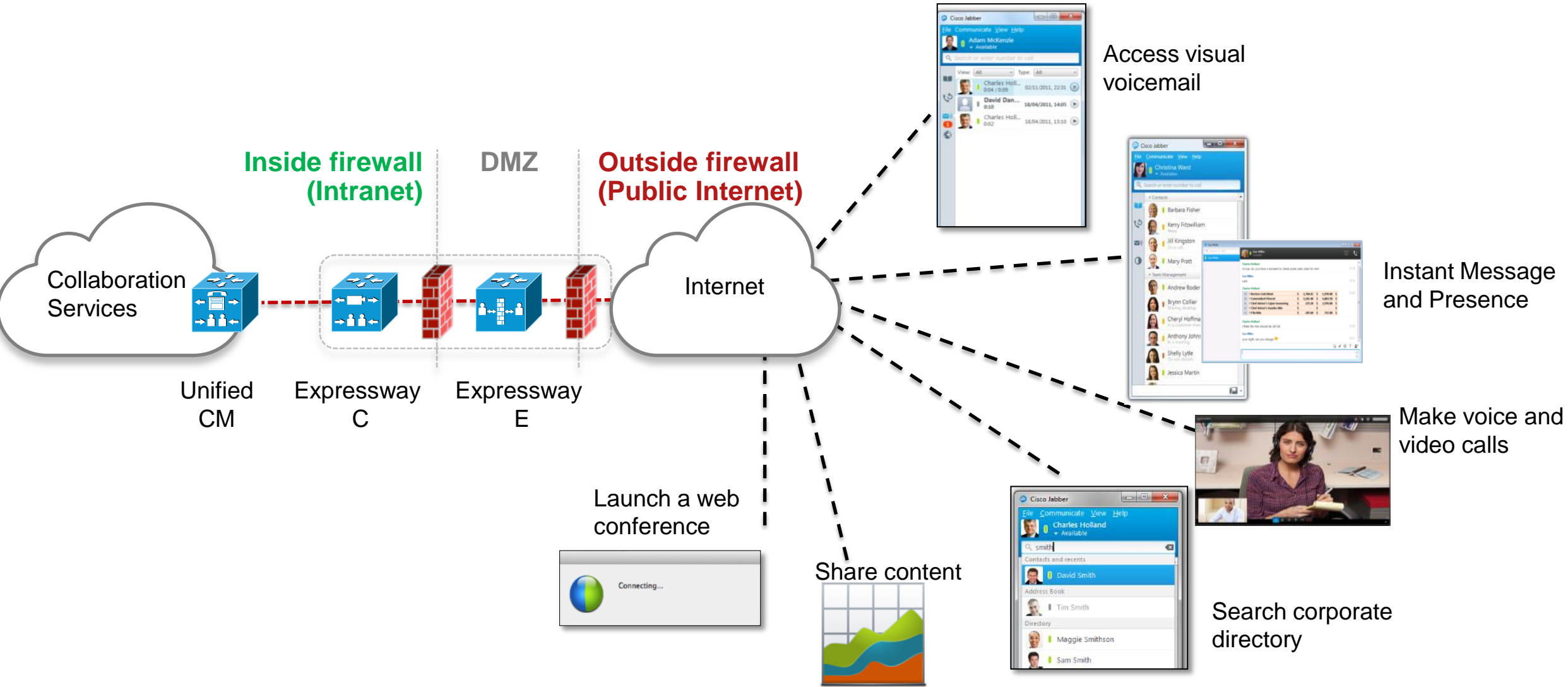
- Mobile and Remote Access

The mobile and remote access solution supports a hybrid on-premise and cloud-based service model, providing a consistent experience inside and outside the enterprise.

It provides a secure connection for Jabber application traffic without having to connect to the corporate network over a VPN.



# What can a Jabber client do with Expressway?



# Software Requirements

- CUCM 9.1(2)SU1 or above
- CUP 9.1(1) or above
- ExpressWay/VCS X8.1.1
- Jabber 9.7 (windows)

# ExpressWay Configuration

# ExpressWay Configuration

## Main configuration steps

1. System configuration
2. Firewall configuration
3. Certificate configuration and deployment
4. Traversal zone configuration
5. UC server discovery
6. DNS and domain configuration/deployment

# Configuration System configuration

- System name and domain must be set for each server
- Each server must have proper DNS configuration

> System > DNS

The screenshot shows the DNS configuration page in a system management interface. The page title is "DNS" and the breadcrumb trail is "You are here: System > DNS".

**DNS settings**

System	<input type="text" value="xway"/>	<a href="#">i</a>
host name		
Domain	<input type="text" value="coluc.com"/>	<a href="#">i</a>
name		
DNS	<input type="text" value="Use the ephemeral port range"/>	<a href="#">i</a>
requests		
port range		

**Default DNS servers**

Address 1	<input type="text" value="10.48.83.51"/>	<a href="#">i</a>
Address 2	<input type="text"/>	<a href="#">i</a>
Address 3	<input type="text"/>	<a href="#">i</a>
Address 4	<input type="text"/>	<a href="#">i</a>
Address 5	<input type="text"/>	<a href="#">i</a>



# Configuration System configuration

- Each system must be synched with NTP server  
> System > Time

The screenshot displays the Cisco TelePresence Video Communication Server Expressway configuration interface. The main navigation bar includes 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The current page is 'Time', with a breadcrumb trail 'System > Time'. The 'NTP servers' section shows five servers configured with addresses from 3.ntp.tandberg.com to 0.ntp.tandberg.com, all with 'Authentication' set to 'Disabled'. The 'Time zone' section shows 'Japan' selected. An inset window titled 'Status (last updated: 13:03:27 JST)' shows the system is 'Synchronized' and provides a detailed table of NTP server status.

NTP server	Condition	Flash	Authentication	Event	Reachability	Offset	Delay	Stratum	Ref ID	Ref time	Dispersion	Jitter	Root delay	Root dispersion
133.27.94.149	candidate	00 ok	none	-	✓✓✓✓✓	0.09 ms	6.253 ms	2	131.113.192.40	Tue, Oct 8 2013 12:31:01.357	0.145 ms	0.055 ms	1.389 ms	0 s
157.7.152.139	sys.peer	00 ok	none	-	✓✓✓✓✓	0.474 ms	1.779 ms	2	133.243.238.243	Tue, Oct 8 2013 13:01:27.817	0.112 ms	0.044 ms	2.258 ms	0 s
218.45.21.199	candidate	00 ok	none	sys_peer	✓✓✓✓✓	-4.32 ms	12.45 ms	2	133.243.238.244	Tue, Oct 8 2013 12:44:10.186	0.164 ms	6.44 ms	7.446 ms	0 s
58.1.228.241	outlyer	00 ok	none	-	✓✓✓✓✓	2.361 ms	6.606 ms	3	165.246.43.195	Tue, Oct 8 2013 12:28:40.221	0.109 ms	0.202 ms	125.9 ms	0 s

# Configuration System Configuration

- If NTP is not configured and synchronized on ExpressWay-C and ExpressWay-E Jabber Telephony registration to CUCM will not succeed.
- Security mechanism based on SIP SERVICE messages.
  1. Expressway-E time-stamps a SERVICE message
  2. Expressway-E sends the SERVICE message to Expressway-C
  3. Expressway-C verifies the SERVICE is received within 60 secs error margin

# Configuration System Configuration

- Enable Mobile and Remote Access  
Configuration > Unified Communications > Configuration



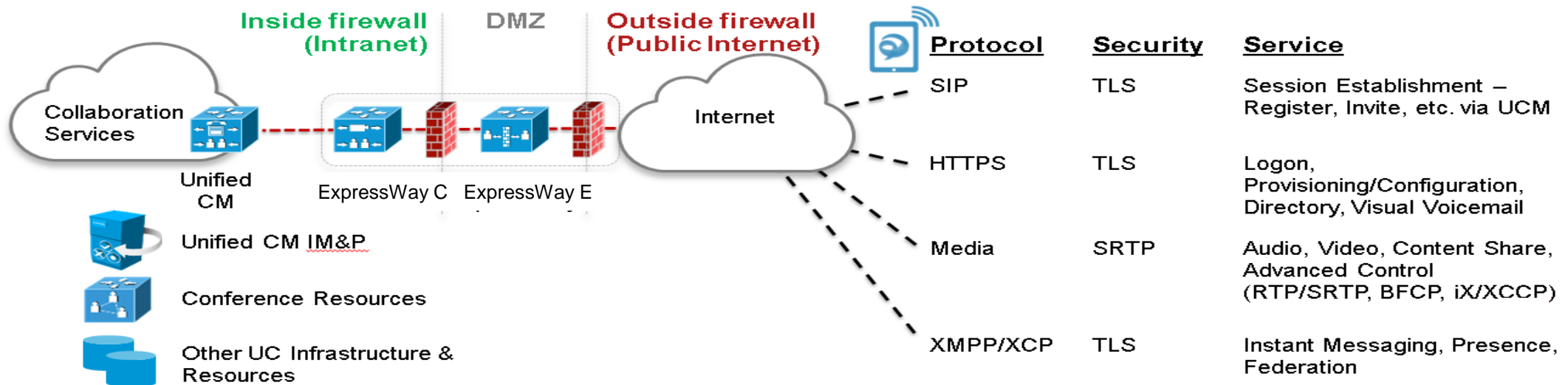
- Check the Administrator guide for more help on system configuration topics



# Firewall Configuration

# Firewall Configuration

- What traffic does the firewall need to pass?
  - ✓ HTTPS proxy for secure provisioning of endpoints
  - ✓ SIP/TLS, RTP/SRTP for audio/video media
  - ✓ XCP/XMPP for IM&P for Jabber
  - ✓ Visual Voicemail (REST/HTTPS)
  - ✓ Traversal Connection between ExpressWay C and E



# Firewall Configuration

## To which ports does this translate?

- Port usage: ExpressWay C to Expressway E



		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
IP Ports	XMPP (IM and Presence)	TCP $U_e$ 30000 to 35999 *	TCP 7400
	SSH (HTTP/S tunnels)	TCP $U_e$ 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & $TLS_A$ 25000 to 29999	TCP & $TLS_B$ 7001
	SIP media	UDP $Y_C$ 36000 to 59999 **	UDP $Y_E$ 36000 to 59999 **

TCP &  $TLS_A$  = Configurable TCP Outbound ports range

TCP &  $TLS_B$  = Configurable traversal port for traversal link between Control and Expressway (i.e. 7001, 7002, etc.)

$U_e$  = Configurable TCP ephemeral port range

$Y_C$  = Configurable traversal media ports range (on Control/C)

$Y_E$  = Configurable traversal media ports range (on Expressway/E)

\* Default ephemeral ports range (X8.1) for is 30000 – 35999 which configurable

\*\* Default media ports range (X8.1) is 36000 – 59999 which configurable

# Firewall Configuration

## Where to configure these ports?


- ExpressWay C

> System > Administration


	ExpressWay C Source Port	ExpressWay E Listening Port
Management Control	Inbound and outbound calls	
Open Firewall	Private to DMZ	
IP Address	IP address of - ExpressWay C	IP address of - ExpressWay E
XMPP (IM and Presence)	TCP $U_e$ 30000 to 35999 *	TCP 7400
SSH (HTTP/S tunnels)	TCP $U_e$ 30000 to 35999 *	TCP 2222
SIP signaling	TCP & $TLS_A$ 25000 to 29999	TCP & $TLS_B$ 7001
SIP media	UDP $Y_C$ 36000 to 59999 **	UDP $Y_E$ 36000 to 59999 **


**System administration**

**System name**

System name  

**Ephemeral port range**

Ephemeral port range start  

Ephemeral port range end  

# Firewall Configuration

## Where to configure these ports?

- ExpressWay C

> Protocols > SIP

	ExpressWay C Source Port	ExpressWay E Listening Port
Management Control	Inbound and outbound calls	
Open Firewall	Private to DMZ	
IP Address	IP address of - ExpressWay C	IP address of - ExpressWay E
XMPP (IM and Presence)	TCP 7400	TCP $U_e$ 30000 to 35999 *
SSH (HTTP/S tunnels)	TCP $U_e$ 30000 to 35999 *	TCP 2222
SIP signaling	TCP & TLS <sub>A</sub> 25000 to 29999	TCP & TLS <sub>B</sub> 7001
SIP media	UDP $Y_c$ 36000 to 59999 **	UDP $Y_e$ 36000 to 59999 **

### SIP

Configuration

SIP mode  ⓘ

UDP mode  ⓘ

UDP port \*  ⓘ

TCP mode  ⓘ

TCP port \*  ⓘ

TLS mode  ⓘ

TLS port \*  ⓘ

TCP outbound port start \*  ⓘ

TCP outbound port end \*  ⓘ



# Firewall Configuration

## Where to configure these ports?

- ExpressWay C

> Configuration > Traversal Subzone

		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control	Inbound and outbound calls		
Open Firewall	Private to DMZ		
IP Address	IP address of - ExpressWay C	IP address of - ExpressWay E	
	XMPP (IM and Presence)	TCP 7400	TCP $U_e$ 30000 to 35999 *
	SSH (HTTP/S tunnels)	TCP $U_e$ 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & $TLS_A$ 25000 to 29999	TCP & $TLS_B$ 7001
	SIP media	UDP $Y_c$ 36000 to 59999 **	UDP $Y_e$ 36000 to 59999 **

**Traversal Subzone**

*i* Saved: Local Zone updated.

**Ports**

Traversal media port start \* 36000 *i*

Traversal media port end \* 59999 *i*

# Firewall Configuration

## Where to configure these ports?

- ExpressWay E Zone

> Configuration > Zone > Traversal

	ExpressWay C Source Port	ExpressWay E Listening Port
Management Control	Inbound and outbound calls	
Open Firewall	Private to DMZ	
IP Address	IP address of - ExpressWay C	IP address of - ExpressWay E
XMPP (IM and Presence)	TCP 7400	TCP $U_e$ 30000 to 35999 *
SSH (HTTP/S tunnels)	TCP $U_e$ 30000 to 35999 *	TCP 2222
SIP signaling	TCP & $TLS_A$ 25000 to 29999	TCP & $TLS_B$ 7001
SIP media	UDP $Y_C$ 36000 to 59999 **	UDP $Y_E$ 36000 to 59999 **

**Edit zone**

SIP

Mode: On

Port: 7001

Transport: TLS

Unified Communications services: Yes

TLS verify mode: On

TLS verify subject name: \*xwayc.coluc.com

Media encryption mode: Force encrypted

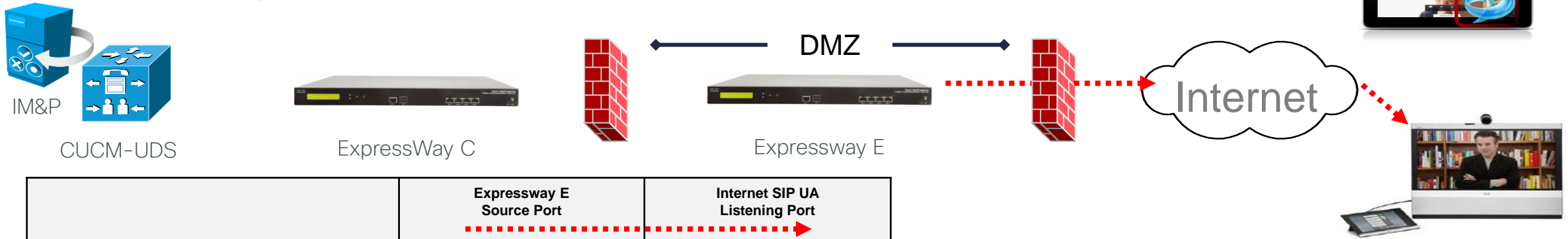
ICE support: Off

Poison mode: Off

# Firewall Configuration

## To which ports does this translate?

- Port usage: Expressway E to/from Public Internet



		Expressway E Source Port	Internet SIP UA Listening Port
Management Control		Outbound to SIP UA in the Internet	
Open Firewall		DMZ to Internet	
IP Address		Public IP address of - ExpressWay E	IP address of - Any (or specific IP)
IP Ports	XMPP (IM and Presence)	N/A	N/A
	UDS (Provisioning and Phonebook)	N/A	N/A
	TURN Server Control	N/A	N/A
	SIP signaling	TLS 25000 to 29999	TLS <b>S</b> >= 1024
	Media	UDP <b>Y<sub>E</sub></b> 36000 to 59999 **	UDP <b>N</b> >= 1024

**N** = ExpressWay wait unit it receives media, then it sends its media to the IP port from which media was received (egress port of the media from the far end non SIP-aware firewall)

**S** = Source port, typically  $\geq 1024$

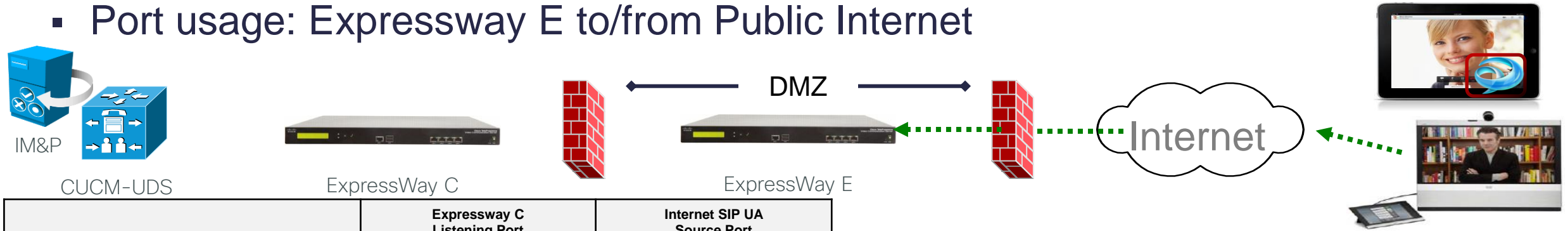
**Y<sub>E</sub>** = Configurable traversal media ports range (on Expressway/E)

\*\* Default media ports range (X8.1) is 36000 – 59999 which configurable

# Firewall Configuration

## To which ports does this translate?

- Port usage: Expressway E to/from Public Internet



		Expressway C Listening Port	Internet SIP UA Source Port
		←	
Management Control		Inbound from SIP UA in the Internet	
Open Firewall		Internet to DMZ	
IP Address		IP address of - VCS Expressway	IP address of - Any (or specific IP)
IP Ports	XMPP (IM and Presence)	TCP 5222	TCP <b>S</b> >= 1024
	UDS (Provisioning)	TCP 8443	TCP <b>S</b> >= 1024
	TURN Server Control	UDP 3478	UDP <b>S</b> >= 1024
	SIP signaling	TLS 5061	TLS <b>S</b> >= 1024
	Media	UDP <b>Y<sub>E</sub></b> 36000 to 59999 **	UDP <b>N</b> >= 1024

**N** = ExpressWay wait unit it receives media, then it sends its media to the IP port from which media was received (egress port of the media from the far end non SIP-aware firewall)

**S** = Source port, typically >=1024

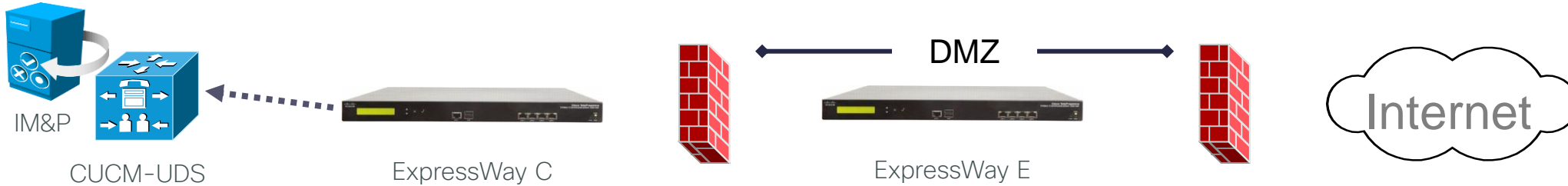
**Y<sub>E</sub>** = Configurable traversal media ports range (on Expressway/E)

\*\* Default media ports range (X8.1) is 36000 – 59999 which configurable

# Firewall Configuration

## To which ports does this translate?

- Port usage: ExpressWay C to Unified CM and IM&P



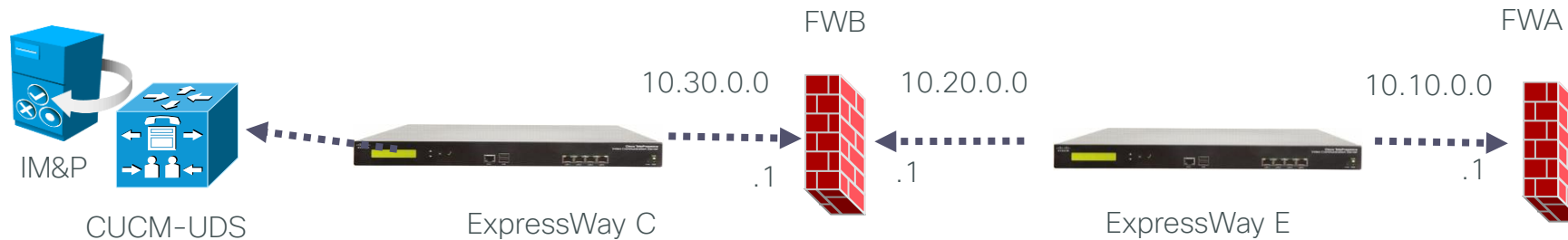
		CUCM&CUP System Listening Port	ExpressWay C Source Port
Management Control		Private Network	
Open Firewall		N/A	
IP Address		IP address of - Unified CM - IM & Presence Server	IP address of - ExpressWay C
IP Ports	XMPP (IM and Presence)	TCP 7400 (IM&P Server)	TCP <b>Ue</b> 30000 to 35999 *
	UDS (Provisioning and Phonebook)	TCP 8443 (CUCM Server)	TCP <b>Ue</b> 30000 to 35999 *
	TFTP	TCP 6970 (TFTP Server)	TCP <b>Ue</b> 30000 to 35999 *
	CUC (Voicemail)	TCP 443 (CUC server)	TCP <b>Ue</b> 30000 to 35999 *

**Ue** = Configurable TCP ephemeral port range

\* Default ephemeral ports range (X8.1) for is 30000 – 35999 which configurable

# Firewall Setup

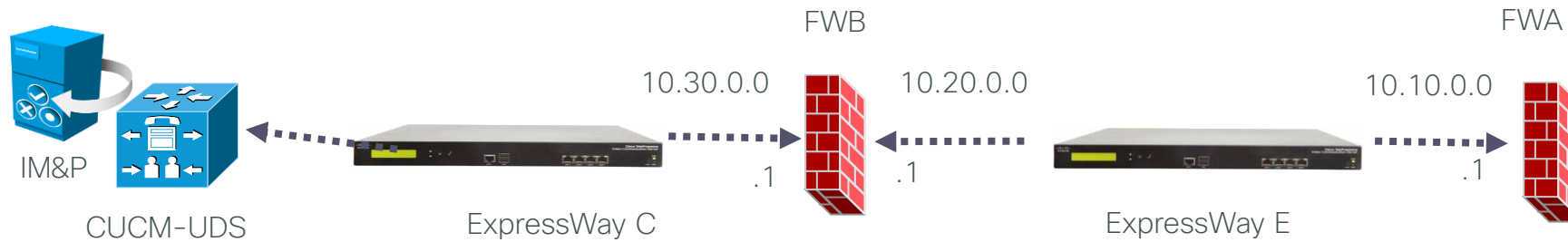
## Dual NIC consideration



- ExpressWay-E has default GTW 10.10.0.1
- When FWB does NAT for 10.30.0.0 there is no problem
- When FWB does no NAT for 10.30.0.0 a static route needs to be added  
xCommand RouteAdd Address: 10.30.0.0 PrefixLength: 24 Gateway: 10.20.0.1 Interface: LAN1

# Firewall Setup

## Dual NIC consideration with static NAT & NAT Reflection



- ExpressWay-C traversal client points to public IP on ExpressWay-E
- FWA must support NAT Reflection

# Firewall Setup

## Port Status and Configuration

- Maintenance > Tools > Port Usage

**Local inbound ports** You are here: [Maintenance](#) > [Tools](#) > [Port usage](#) > Local inbound ports

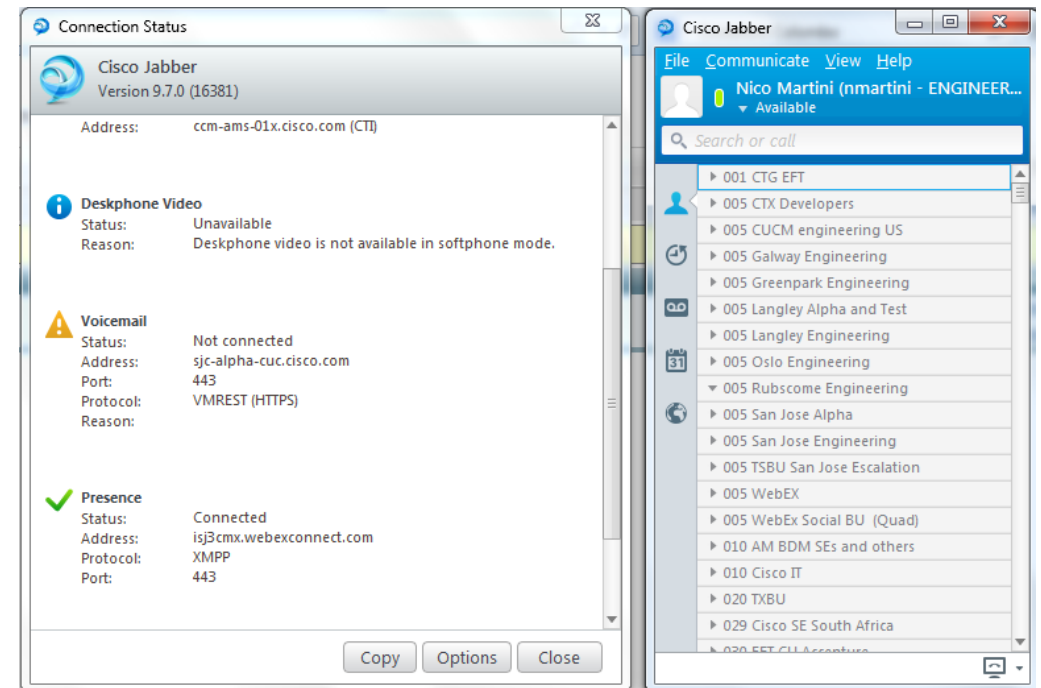
Type	Description	Protocol	IP address	IP port	Transport	Actions
Administration	SSH port		10.48.55.99	22	TCP	Not configurable
Administration	HTTP port		10.48.55.99	80	TCP	Not configurable
Administration	HTTPS port		10.48.55.99	443	TCP	Not configurable
Administration	SNMP port		10.48.55.99	161	UDP	Not configurable
H.323	Multicast gatekeeper discovery port	H.323	10.48.55.99	1718	UDP	Not configurable
H.323	Call signaling TCP port	H.323	10.48.55.99	1720	TCP	<a href="#">View/Edit</a>
H.323	Call signaling port range	H.323	10.48.55.99	15000-19999	TCP	<a href="#">View/Edit</a>
H.323	Registration UDP port	H.323	10.48.55.99	1719	UDP	<a href="#">View/Edit</a>
SIP	TCP port	SIP	10.48.55.99	5060	TCP	<a href="#">View/Edit</a>
SIP	TLS port	SIP	10.48.55.99	5061	TCP	<a href="#">View/Edit</a>
Media	Media port range	RTP,RTCP	10.48.55.99	50000-54999	UDP	<a href="#">View/Edit</a>
Expressway	H.323 Assent call signaling port	H.323	10.48.55.99	2776	TCP	<a href="#">View/Edit</a>
Expressway	H.323 H.460.18 call signaling port	H.323	10.48.55.99	2777	TCP	<a href="#">View/Edit</a>
Traversal server zone	TraversalZone	SIP	10.48.55.99	7001	TCP	<a href="#">View/Edit</a>
Unified Communications	SSH tunnels	SSH	10.48.55.99	2222	TCP	Not configurable
Unified Communications	HTTP proxy	HTTP	10.48.55.99	8443	TCP	Not configurable
Unified Communications	XMPP proxy client port	XMPP	10.48.55.99	5222	TCP	Not configurable
Unified Communications	XMPP proxy router port	XMPP	10.48.55.99	7400	TCP	Not configurable

[Export to CSV](#)



# HTTP Server Allow list ExpressWay C

- Some services are relying on HTTP Reverse Proxy functionality in Expressways  
Example :
  - “Unity Connection Voicemail Player”
  - “Customized Jabber HTTP Contact Photos”
  - “Customizes Jabber plugins”



# HTTP Server Allow list ExpressWay C

- > Configuration > Unified Communications > Configuration

HTTP server allow list	
Server hostname	Description
<input type="checkbox"/> <a href="#">Train.eft.cisco.com</a>	TRAIN BOOKING SERVICE
<input type="checkbox"/> <a href="#">Photos.eft.cisco.com</a>	HTTP PHOTO REPOSITORY
<input type="checkbox"/> <a href="#">voicemail.eft.cisco.com</a>	VOICEMAIL SERVER

- The hostname or IP address of an HTTP server that a Jabber client located outside of the enterprise is allowed to access.

Access is granted if the server portion of the client-supplied URI matches the name entered here, or if it resolves via DNS lookup to an IP address specified here.



# Certificates

# Certificates

- Maintenance > Security Certificate > Server Certificate

**Server certificate** You are here: [Maintenance](#) > [Security certificates](#) > Server certificate

**Server certificate data**

Server certificate

Currently loaded certificate expires on Mar 24 2015

**Certificate signing request (CSR)**

Certificate request There is no certificate signing request in progress

**Upload new certificate**

Select the server private key file  No file chosen

Select the server certificate file  No file chosen

# Certificates

- Maintenance > Security Certificate > Trusted CA Certificate


**Trusted CA certificate** You are here: [Maintenance](#) > [Security certificates](#) > [Trusted CA certificate](#)

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=CISCO, OU=TAC, CN=MACOS	Matches Issuer	Apr 23 2014	Valid	<a href="#">View (decoded)</a>

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

---

**Upload**

Select the file containing trusted CA certificates [Choose File](#) No file chosen 

[Append CA certificate](#) [Reset to default CA certificate](#)

# ExpressWay C – Certificate Requirements

- CA Signed
  - Must be CA signed
  - Used with ExpressWay E for traversal zone connection
  - Used with CUCM when endpoint security mode is Authenticated or Encrypted (TLS transport used)
  - CA Root must be appended to “Trusted CA certificate” on both ExpressWay’s
  - CA Root must be uploaded to Callmanager-trust store on every node in the cluster

# ExpressWay C – Certificate Requirements

## CA Root not uploaded on ExpressWay E

- Traversal Zone State **Failed**

Status	
State	Failed
SIP port	Active
H.323 port	Inactive
Cause	System unreachable
Number of calls to this zone	0
Bandwidth used on this Expressway	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

**Related tasks**

- [Configure search rules](#)

- Expressway-C Diagnostics logs (traversal client)

```
xwayc tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25016" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="xwaye.coluc.com" Level="1" UTCTime="2014-03-24 17:33:30,872"
```

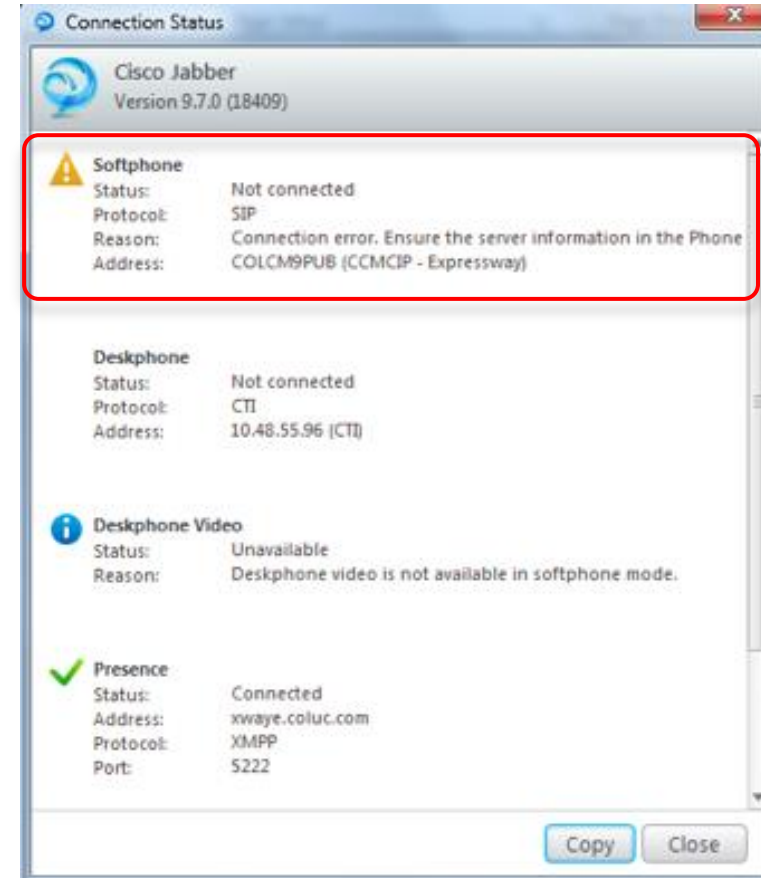
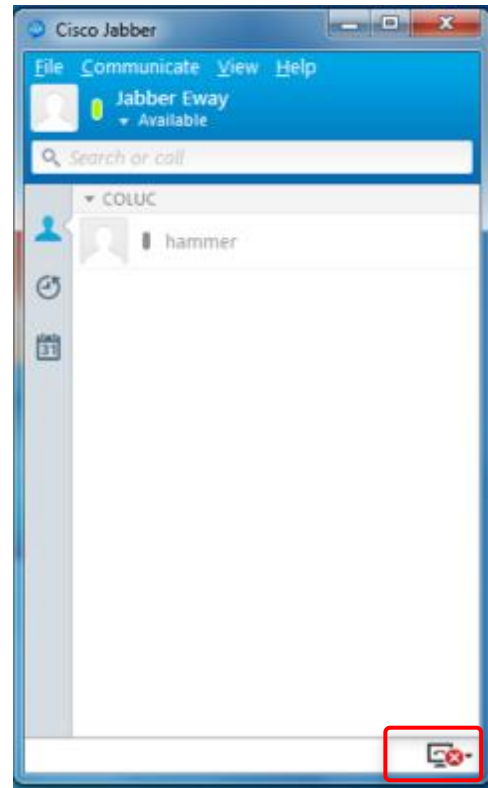
- Expressway Event logs

Results	
2014-03-24T17:36:30+00:00	tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25025" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="xwaye.coluc.com" Level="1" UTCTime="2014-03-24 17:36:30,872"

# ExpressWay C - Certificate Requirements

## CA Root not uploaded on CUCM

- Softphone Registration fails (other will work) when endpoint security settings are authenticated or encrypted





# ExpressWay C – Certificate Requirements

- SAN must include 'Chat node alias' from IM&P server (CUP)
  - Required for XMPP federation
  - Get auto-added in CSR after IM&P discovery
  - For manual configuration go to CUPADMIN > Messaging > Group Chat Server Alias Mapping, click find.

# ExpressWay C – Certificate Requirements

CUPADMIN > Messaging > Group Chat Server Alias Mapping

**Generate CSR** You are here: [Maintenance](#) > [Security certificates](#) > Generate CSR

**Common name**

Common name: FQDN of Expressway

Common name as it will appear: xwayc.coluc.com

**Alternative name**

Additional alternative names (comma separated):

IM and Presence chat node aliases: **conference-2-ecup9.coluc.com**

Unified CM phone security profile names: csf-secure

Alternative name as it will appear: xwayc.coluc.com,conference-2-ecup9.coluc.com,csf-secure

**Additional information**

Key length (in bits): 4096

Country: \* BE

State or province: \* BRABANT

Locality (town name): \* DIEGEM

Organization (company name): \* CISCO

Organizational unit: \* TAC

Generate CSR

**Primary Group Chat Server Aliases**

Primary Group Chat Server Alias	Node Name
conference-2-ecup9.coluc.com	ecup.coluc.com

**Group Chat Server Alias** Rows per Page: 50

Find Group Chat Server Alias where Group Chat Server Alias begins with [ ] Find Clear Filter [+] [-]

No active query. Please enter your search criteria using the options above.

Add New

**Group Chat Server Alias (1 - 1 of 1)** Rows per Page: 50

<input type="checkbox"/>	Group Chat Server Alias	Node Name
<input type="checkbox"/>	conference-2-ecup9.coluc.com	ecup.coluc.com

Add New Select All Clear All Delete Selected

# ExpressWay C – Certificate Requirements

- SAN must include ‘Device Security Profile Name’
  - Required for CUCM to accept the TLS Connection
  - X509 from certificate presented is that one of ExpressWay C
  - CUCM needs to validate using SAN matching the security profile name
  - Some (public) CA’s do not allow hostname in SAN  
If so, the profile name must have FQDN format

# ExpressWay C – Certificate Requirements

**Generate CSR** You are here: [Maintenance](#) > [Security certificates](#) > Generate CSR

**Common name**

Common name	FQDN of Expressway
Common name as it will appear	xwayc.coluc.com

**Alternative name**

Additional alternative names (comma separated)	<input type="text"/>
IM and Presence chat node aliases	<input type="text" value="conference-2-ecup9.coluc.com"/>
Unified CM phone security profile names	<input type="text" value="csf-secure"/>
Alternative name as it will appear	xwayc.coluc.com,conference-2-ecup9.coluc.com,csf-secure


**Additional information**

Key length (in bits)	<input type="text" value="4096"/>
Country	<input type="text" value="BE"/>
State or province	<input type="text" value="BRABANT"/>
Locality (town name)	<input type="text" value="DIEGEM"/>
Organization (company name)	<input type="text" value="CISCO"/>
Organizational unit	<input type="text" value="TAC"/>

Generate CSR

## System > Security > Phone Security Profile

**Status**

 Status: Ready

---

**Phone Security Profile Information**

**Product Type:** Cisco Unified Client Services Framework

**Device Protocol:** SIP

**Name \***

**Description**

**Device Security Mode**

**Transport Type \***

TFTP Encrypted Config

---

**Phone Security Profile CAPF Information**

**Authentication Mode \***

**Key Size (Bits) \***

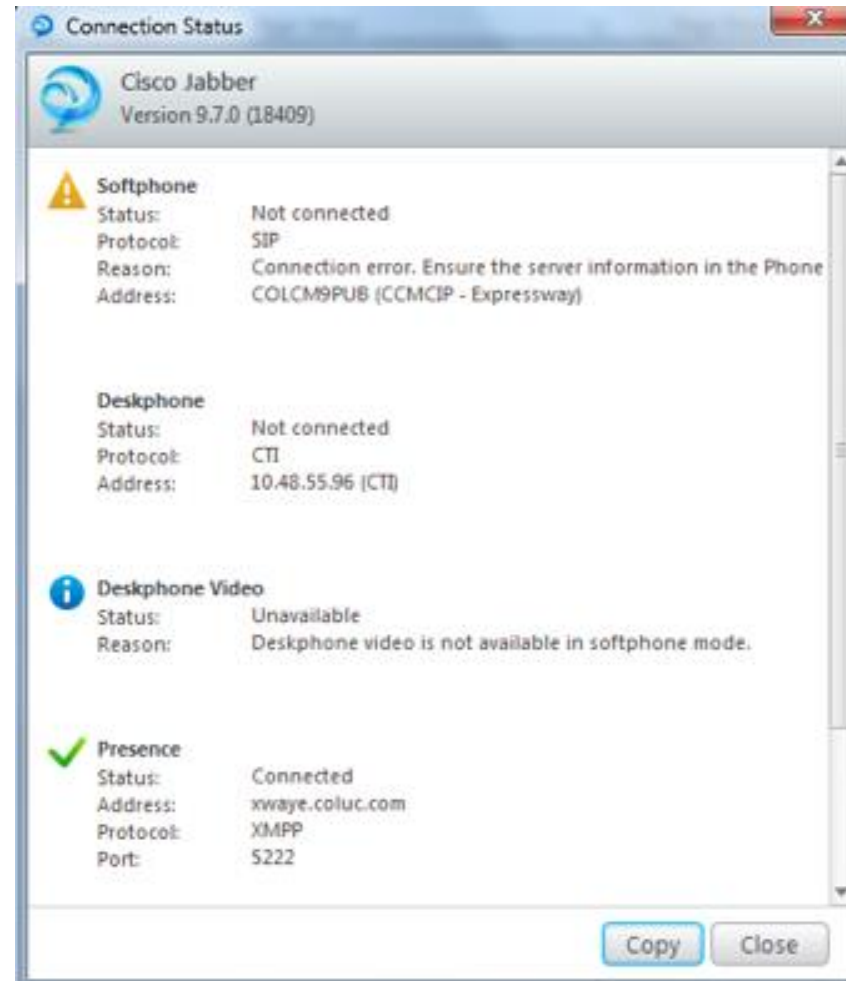
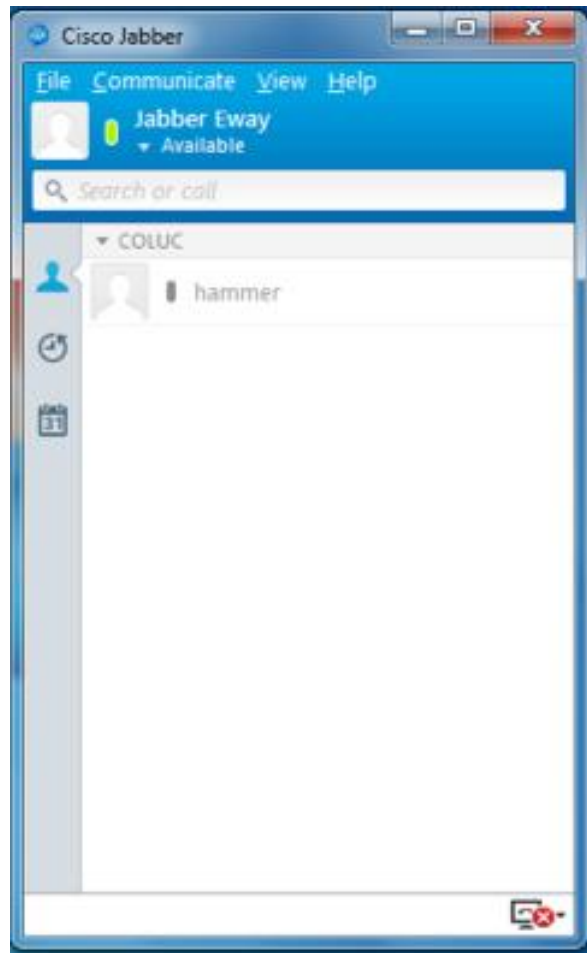
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

---

**Parameters used in Phone**

**SIP Phone Port \***

# ExpressWay C – Certificate Requirements Security Profile not added as SAN



# ExpressWay E – Certificate Requirements

- CA Signed
  - Must be CA signed
  - Used with ExpressWay C for traversal zone connection
  - CA Root must be appended to “Trusted CA certificate” on both ExpressWay’s

# ExpressWay E – Certificate Requirements

## CA root not uploaded to ExpressWay C

- Traversal Zone State

Status	
State	Failed
SIP port	Active
H.323 port	Inactive
Cause	System unreachable
Number of calls to this zone	0
Bandwidth used on this Expressway	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

**Related tasks**

[Configure search rules](#)

- ExpressWay E diagnostic logs

xway tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25006" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Level="1" UTCTime="2014-03-25 09:52:36,680"

- ExpressWay E event logs

Results	
2014-03-25T09:54:16+00:00	tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25011" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Level="1" UTCTime="2014-03-25 09:54:16,676"

# Common

- If Expressway does not have a valid signed certificate that contains either the FQDN or domain of Expressway, then this fails and the Jabber client fails to log in.
- If this issue occurs, the customer should use the Certificate Signing Request (CSR) tool on Expressway, which automatically includes the FQDN of Expressway as a Subject Alternative Name (SAN).
- *Expressway-C Server Certificate Requirements:*
- The **Chat Node Aliases** configured on the IM&P servers. This is required if you perform Extensible Messaging and Presence Protocol (XMPP) federation. Expressway-C should automatically include these in the CSR provided that an IM&P server has already been discovered on Expressway-C.
- The names in FQDN format of all **Phone Security Profiles** in CUCM configured for TLS and used on devices configured for MRA. This allows for secure communication between the CUCM and Expressway-C for the devices that use those Phone Security Profiles.
- *Expressway-E Server Certificate Requirements:*
- All domains configured for Unified Communications. This includes the domain of Expressway-E and C, email address domain configured for Jabber, and any Presence domains.
- The **Chat Node Aliases** configured on the IM&P servers. This is required if you perform XMPP federation.



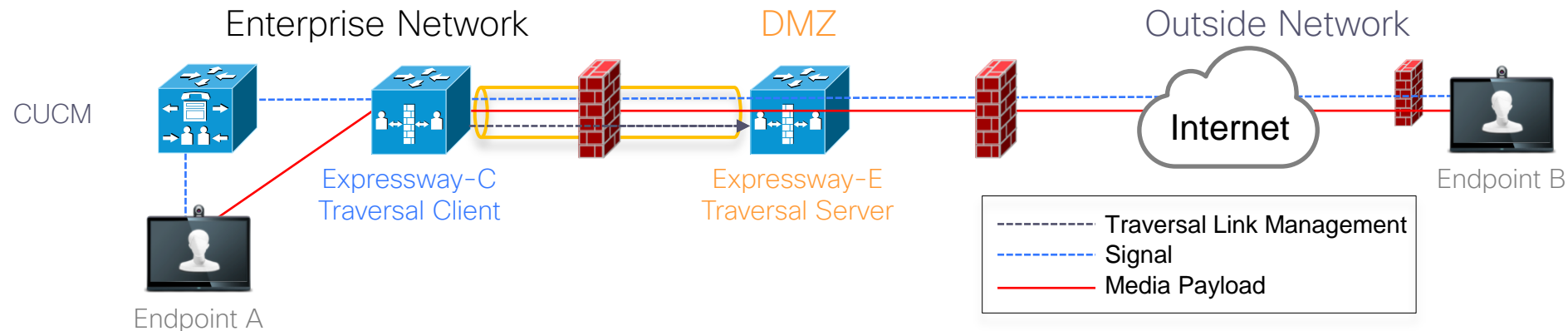


# Traversal Zone Setup

# Traversal Zone Setup

## Firewall Traversal

- Expressway-E is traversal server in DMZ
- Expressway-C is traversal client inside the network
- Establish traversal link between both using traversal zone configuration



# Traversal Zone Setup

## ExpressWay E – Traversal Server

**Configuration**

Name	★ Traversal Zone ⓘ
Type	Unified Communications traversal
Hop count	★ 15 ⓘ

Select Type : Unified Communications traversal

**Connection credentials**

Username	★ traversal ⓘ
Password	<a href="#">Add/Edit local authentication database</a>

Configure username to be used by Traversal Client to authenticate with server

# Traversal Zone Setup

## ExpressWay E – Traversal Server

**SIP**

Port	<input type="text" value="7001"/>
TLS verify subject name	<input type="text" value="expressc.cloud.com"/>
Accept proxied registrations	<input type="text" value="Allow"/>
ICE support	<input type="text" value="Off"/>
SIP poison mode	<input type="text" value="Off"/>

Port is default 7001, listening port for traversal client connection

Must match CN from Certificate presented by Traversal Client (ExpressWay C)

**Authentication**

Authentication policy	<input type="text" value="Do not check credentials"/>
-----------------------	---

Must be set to 'Do not check ..'

(expressway does not register any endpoint)

**UDP / TCP probes**

UDP retry interval	<input type="text" value="2"/>
UDP retry count	<input type="text" value="5"/>
UDP keep alive interval	<input type="text" value="20"/>
TCP retry interval	<input type="text" value="2"/>
TCP retry count	<input type="text" value="5"/>
TCP keep alive interval	<input type="text" value="20"/>

# Traversal Zone Setup

## ExpressWay C – Traversal Client

**Configuration**

Name	* <input type="text" value="Traversal Zone"/>	<i>i</i>
Type	<input type="text" value="Unified Communications traversal"/>	
Hop count	* <input type="text" value="15"/>	<i>i</i>

→ Type: Unified Communication traversal

**Connection credentials**

Username	* <input type="text" value="traversal"/>	<i>i</i>
Password	* <input type="password" value="*****"/>	<i>i</i>

→ Configure same username and password as added on the Traversal Server (Expressway E)

# Traversal Zone Setup

## ExpressWay C – Traversal Client

**SIP**

Port \*  ⓘ

Accept proxied registrations  ⓘ

ICE support  ⓘ

SIP poison mode  ⓘ

Destination port Traversal Server is listening on

**Authentication**

Authentication policy  ⓘ

Must be set to 'Do not check ..'  
(expressway does not register any endpoint)


**Client settings**

Retry interval \*  ⓘ

# Traversal Zone Setup

## ExpressWay C – Traversal Client

**Location**



Peer 1 address	<input type="text" value="expresse.cloud.com"/>		SIP: Reachable: 10.75.63.71:7001
Peer 2 address	<input type="text"/>		

- 
- Must be FQDN
  - Must be DNS resolvable

# Traversal Zone Setup

## Peer Address not matching CN

- Peer Address configured as IP address

Location	
Peer 1 address	<input type="text" value="10.48.55.99"/> 
Peer 2 address	<input type="text"/> 

SIP: Failed to connect to 10.48.55.99:7001 :  
TLS negotiation failure

- ExpressWay diagnostic logs

```
2014-03-25T14:08:16+00:00 xwayc tvcs: Event="Outbound TLS Negotiation Error"  
Service="SIP" Src-ip="10.48.55.98" Src-port="25697" Dst-ip="10.48.55.99" Dst-port="7001"  
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-  
name="10.48.55.99" Level="1" UTCTime="2014-03-25 14:08:16,699"
```

- ExpressWay Event logs

Results
2014-03-25T14:09:56+00:00 tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25702" Dst-ip="10.48.55.99" Dst-port="7001" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.55.99" Level="1" UTCTime="2014-03-25 14:09:56,698"



# Traversal Zone Setup

## Peer Address not matching CN

- Peer Address/FQDN not matching CN

Location

Peer 1 address   SIP: Failed to connect to 10.48.55.99:7001 : TLS negotiation failure

- ExpressWay diagnostic logs

```
2014-03-25T14:16:36+00:00 xwayc tvcs: Event="Outbound TLS Negotiation Error"
Service="SIP" Src-ip="10.48.55.98" Src-port="25714" Dst-ip="10.48.55.99" Dst-port="7001"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-
name="xwy.coluc.com" Level="1" UTCTime="2014-03-25 14:16:36,699"
```

- ExpressWay Event logs

Results

```
2014-03-25T14:09:56+00:00 tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25702" Dst-ip="10.48.55.99"
Dst-port="7001" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.55.99"
Level="1" UTCTime="2014-03-25 14:09:56,698"
```

# Traversal Zone Setup

## Password incorrect

- Traversal Client will show for this zone



- ExpressWay C diagnostic logs

```
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="xwaye.coluc.com" Type="A and AAAA"  
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4"TCP"10.48.55.99'] (A/AAAA) Number of  
relevant records retrieved: 1"  
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99" Dst-port="7001"  
Detail="TCP Connecting"  
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99" Dst-port="7001"  
Detail="TCP Connection Established"
```

....

# Password incorrect

- ExpressWay C event log

```
Results
2014-03-25T14:19:56+00:00 tvcs: Event="External Server Communications Failure" Reason="gatekeeper timed out" Service="NeighbourGatekeeper" Dst-ip="10.48.55.99" Dst-port="7001" Detail="name:xwaye.coluc.com" Protocol="TCP" Level="1" UTCTime="2014-03-25 14:19:56,705"
```

- ExpressWay E event log

```
Results
2014-03-25T14:36:56+00:00 tvcs: Event="Authentication Failed" Service="SIP" Src-ip="10.48.55.98" Src-port="25723" Detail="Incorrect authentication credential for user" Protocol="TLS" Method="OPTIONS" Level="1" UTCTime="2014-03-25 14:36:56,694"
```



# UC Server Discovery

# UC Server Discovery

## Configuration > Unified Communications

**Unified Communications** You are here: [Configuration](#) > [Unified Communications](#) > Configuration

**Configuration**

Unified Communications mode: Mobile and remote access ⓘ

**IM and Presence servers and Unified CM servers**

IM and Presence servers      1 [Discover IM and Presence servers](#)

Unified CM servers            2 [Configure Unified CM servers](#)

**Advanced**

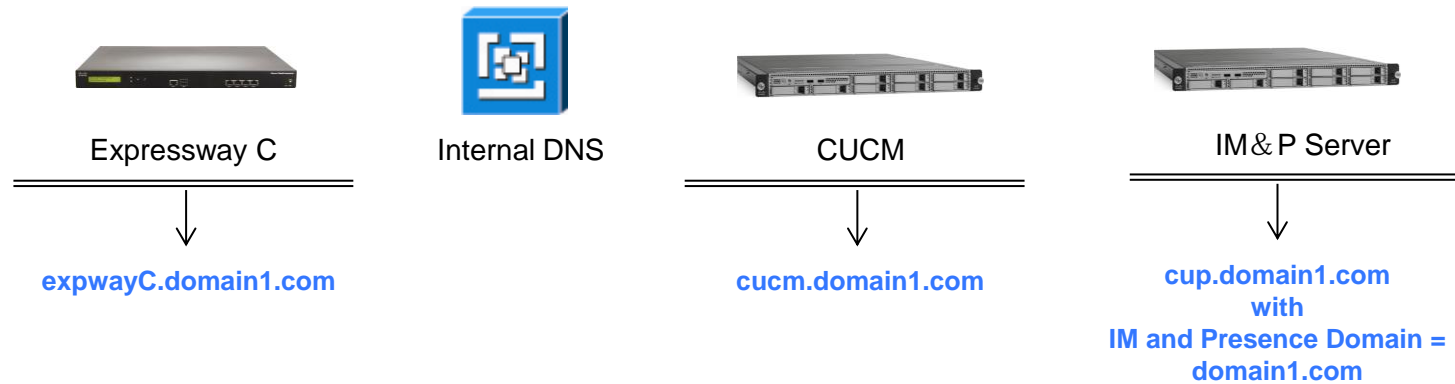
HTTP server allow list      [Configure HTTP server allow list](#)

Advanced settings            [Show advanced settings](#)

**Save**

# ExpressWay – Mobile and Remote Access UC Server discovery

- Scenario 1
  - CUCM set to none-secure



# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery



**Unified CM servers** You are here: [Configuration](#) > [Unified CM servers](#)

**Unified CM server lookup**

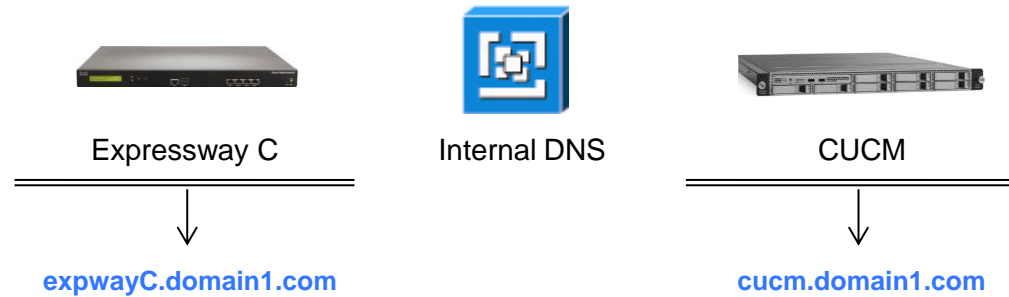
Unified CM publisher address	<input type="text" value="COLCM9PUB.coluc.com"/>	<a href="#">?</a>
Username	<input type="text" value="ccmadmin"/>	<a href="#">?</a>
Password	<input type="password" value="....."/>	<a href="#">?</a>
TLS verify mode	<input type="text" value="Off"/>	<a href="#">?</a>
Deployment	<input type="text" value="Default deployment"/>	<a href="#">?</a>

What do I enter here?

- When TLS verify mode is On > Must match CN from Tomcat Certificate
- When TLS verify mode Off > IP Address Publisher or Hostname Publisher or FQDN Publisher

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery



### Unified CM servers

Unified CM server lookup

Unified CM publisher address: \* COLCM9PUB.coluc.com ⓘ

Username: \* ccmadmin ⓘ

Password: \* ..... ⓘ

TLS verify mode: Off ⓘ

Deployment: Default deployment ⓘ

You are here: Configuration > Unified CM servers > Unified CM server lookup

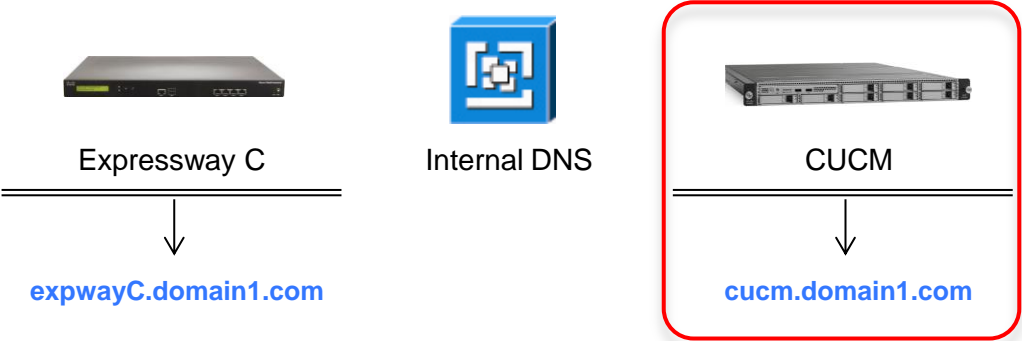
Set to off for non-secure  
When set to 'On'  
what other configuration is required?

- Self Signed Tomcat Certificate must be appended to "Trusted CA Cert"
- Or
- CA certificate must be appended (And address must match CN from Tomcat certificate)



# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery



How does Server configuration on CUCM impact the discovery?

**Servers (1 - 2 of 2)** Rows per Page 50

Find Servers where

<input type="checkbox"/>	Host Name/IP Address ^	Description
<input type="checkbox"/>	<u>COLCM9PUB</u>	COLCM9PUB
<input type="checkbox"/>	<u>COLCM9SUB1</u>	COLCM9SUB1

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery

**Currently found Unified CM nodes**

Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB	TCP	9.1.2	TCP: Active
COLCM9PUB.coluc.com	COLCM9SUB1	TCP	9.1.2	TCP: Active

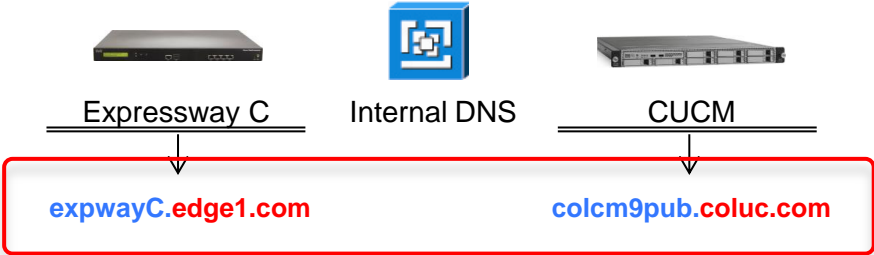
**Servers (1 - 2 of 2)**

Host Name/IP Address	Description
<a href="#">COLCM9PUB</a>	COLCM9PUB
<a href="#">COLCM9SUB1</a>	COLCM9SUB1

- When hostname is returned shows Active when xway can DNS resolve <hostname>@<domain Xway> or <hostname> where <hostname> is what is configured in CCMADMIN
- This creates a problem when Expressway/VCS and CUCM servers are in different domains

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery – Different Server Domain



Servers (1 - 2 of 2) Rows per Page 50

Find Servers where Host Name/IP Address begins with Find Clear Filter

	Host Name/IP Address	Description
<input type="checkbox"/>	COLCM9PUB	COLCM9PUB
<input type="checkbox"/>	COLCM9SUB1	COLCM9SUB1

Unified CM server lookup

Unified CM publisher address: COLCM9PUB.coluc.com

Username: ccmadmin

Password: .....

TLS verify mode: On

Save Delete Cancel

DNS query fails for colcm9pub.edge.com  
colcm9pub

Currently found Unified CM nodes

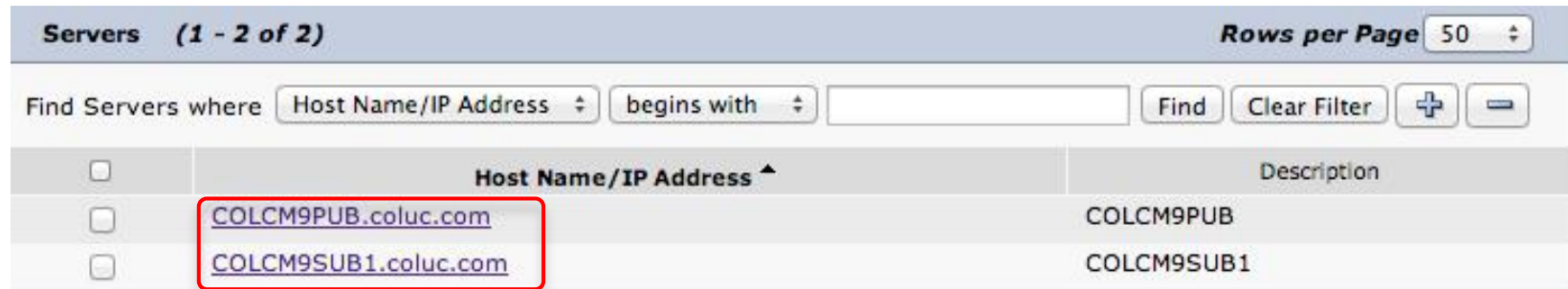
Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB	TCP	9.1.2	TCP: Failed
COLCM9PUB.coluc.com	COLCM9SUB1	TCP	9.1.2	TCP: Failed

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery

- How to solve?

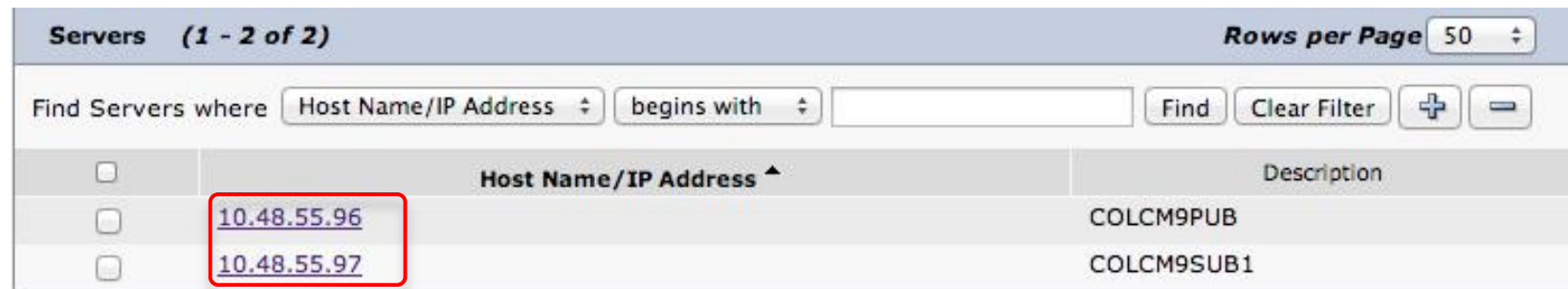
1) Use FQDN for server configuration on CCMADMIN



The screenshot shows the 'Servers' page in CCMADMIN. The search criteria are set to 'Host Name/IP Address' and 'begins with'. The search results table has two rows, both of which are highlighted with a red box. The first row shows the FQDN 'COLCM9PUB.coluc.com' and the second row shows 'COLCM9SUB1.coluc.com'. The descriptions are 'COLCM9PUB' and 'COLCM9SUB1' respectively.

Servers (1 - 2 of 2)		Rows per Page 50
Find Servers where Host Name/IP Address begins with		
	Host Name/IP Address	Description
<input type="checkbox"/>	<a href="#">COLCM9PUB.coluc.com</a>	COLCM9PUB
<input type="checkbox"/>	<a href="#">COLCM9SUB1.coluc.com</a>	COLCM9SUB1

2) Use IP address for server configuration on CCMADMIN



The screenshot shows the 'Servers' page in CCMADMIN. The search criteria are set to 'Host Name/IP Address' and 'begins with'. The search results table has two rows, both of which are highlighted with a red box. The first row shows the IP address '10.48.55.96' and the second row shows '10.48.55.97'. The descriptions are 'COLCM9PUB' and 'COLCM9SUB1' respectively.

Servers (1 - 2 of 2)		Rows per Page 50
Find Servers where Host Name/IP Address begins with		
	Host Name/IP Address	Description
<input type="checkbox"/>	<a href="#">10.48.55.96</a>	COLCM9PUB
<input type="checkbox"/>	<a href="#">10.48.55.97</a>	COLCM9SUB1

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
<input type="checkbox"/> COLCM9PUB.coluc.com	ccmadmin	On	COLCM9SUB1.coluc.com, COLCM9PUB.coluc.com	<a href="#">View/Edit</a>

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

Currently found Unified CM nodes				
Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB.coluc.com	TCP	9.1.2	TCP: Active
COLCM9PUB.coluc.com	COLCM9SUB1.coluc.com	TCP	9.1.2	TCP: Active

When FQDN is returned shows 'Active' when xway can DNS resolve <hostname>@<domain> as configured in CCMADMIN

Here colcm9pub.coluc.com and colcm9sub1.coluc.com

Servers (1 - 2 of 2)		Rows per Page
Find Servers where <input type="text" value="Host Name/IP Address"/> <input type="text" value="begins with"/>		<input type="button" value="Find"/> <input type="button" value="Clear Filter"/>
<input type="checkbox"/>	Host Name/IP Address	Description
<input type="checkbox"/>	COLCM9PUB.coluc.com	COLCM9PUB
<input type="checkbox"/>	COLCM9SUB1.coluc.com	COLCM9SUB1

# ExpressWay Mobile and Remote Access – Scenario 1

## CUCM Server Discovery

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
<input type="checkbox"/> COLCM9PUB.coluc.com	ccmadmin	On	10.48.55.97, 10.48.55.96	<a href="#">View/Edit</a>

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

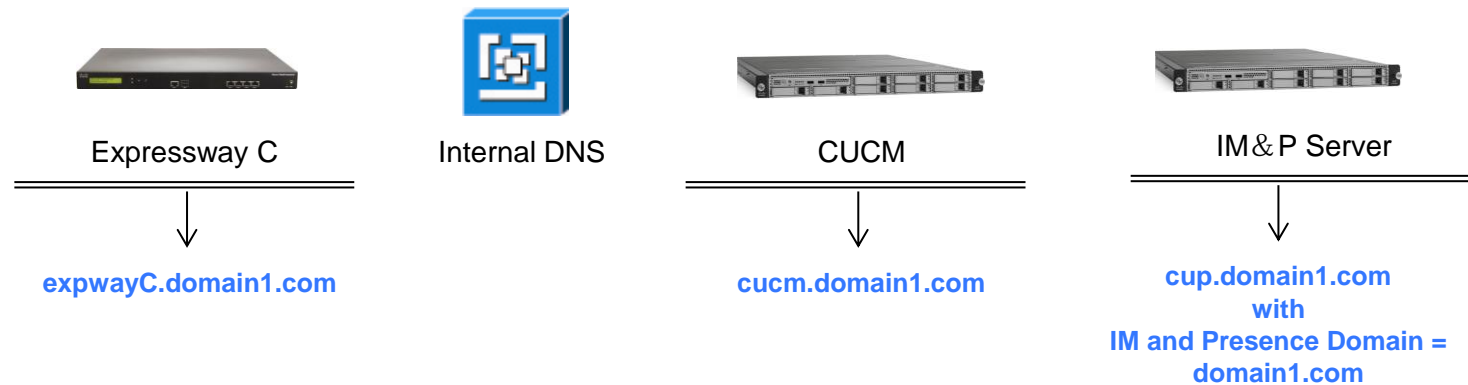
Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	10.48.55.96	TCP	9.1.2	TCP: Active
COLCM9PUB.coluc.com	10.48.55.97	TCP	9.1.2	TCP: Active

No DNS query is required as IP address is used.  
Will always show Active

Servers (1 - 2 of 2)		Rows per Page
Find Servers where		Host Name/IP Address ▾ begins with ▾ <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/> <input type="button" value="+"/> <input type="button" value="-"/>
<input type="checkbox"/>	Host Name/IP Address ^	Description
<input type="checkbox"/>	<a href="#">10.48.55.96</a>	COLCM9PUB
<input type="checkbox"/>	<a href="#">10.48.55.97</a>	COLCM9SUB1

# ExpressWay – Mobile and Remote Access UC Server discovery

- Scenario 2
  - CUCM set to secure (mixed-mode)



# ExpressWay – Mobile and Remote Access

## UC Server discovery

- What does change when CUCM cluster is set to mixed mode?
  - Same steps need to be followed
  - Status will show 'TLS/TCP'

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
<input type="checkbox"/> COLCM9PUB.coluc.com	ccmadmin	On	COLCM9SUB1, COLCM9PUB	<a href="#">View/Edit</a>

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

Currently found Unified CM nodes				
Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB	TLS / TCP	9.1.2	TLS: Active, TCP: Active
COLCM9PUB.coluc.com	COLCM9SUB1	TLS / TCP	9.1.2	TLS: Active, TCP: Active



# ExpressWay – Mobile and Remote Access

## UC Server discovery

- TLS and TCP zone is auto-added per discovered node  
These are Non-configurable neighbor zones “CEtcp-<UCMName>” or/and “CEtls-<UCMName>”

**Zones** You are here: [Configuration](#) > [Zones](#)

Name ▾	Type	Calls	Bandwidth used	H323 status	SIP status	Search rule status	Actions
<a href="#">DefaultZone</a>	Default zone	0	0 kbps	On	On		<a href="#">View/Edit</a>
<a href="#">CEtcp-COLCM9PUB</a>	Neighbor	0	0 kbps	Off	Active	Enabled <a href="#">search rules: 1</a>	<a href="#">View</a>
<a href="#">CEtcp-COLCM9SUB1</a>	Neighbor	0	0 kbps	Off	Active	Enabled <a href="#">search rules: 1</a>	<a href="#">View</a>
<a href="#">CEtls-COLCM9PUB</a>	Neighbor	0	0 kbps	Off	Active	Enabled <a href="#">search rules: 1</a>	<a href="#">View</a>
<a href="#">CEtls-COLCM9SUB1</a>	Neighbor	0	0 kbps	Off	Active	Enabled <a href="#">search rules: 1</a>	<a href="#">View</a>
<input type="checkbox"/> <a href="#">TraversalZone</a>	Traversal client	0	0 kbps	Off	Active	No <a href="#">search rules</a> configured	<a href="#">View/Edit</a>

# ExpressWay – Mobile and Remote Access

## UC Server discovery

**Configuration**

Name: \*CEtcp-COLCM9PUB ⓘ

Type: Neighbor

Hop count: 15 ⓘ

**H.323**

Mode: Off ⓘ

**SIP**

Mode: On ⓘ

Port: \*5060 ⓘ

Transport: TCP ⓘ

Media encryption mode: Auto ⓘ

ICE support: Off ⓘ

**Authentication**

Authentication policy: Treat as authenticated ⓘ

SIP authentication trust mode: Off ⓘ

**Location**

Peer 1 address: COLCM9PUB ⓘ SIP: Reachable: 10.48.55.96:5060

Peer 2 address: ⓘ ⓘ

**Configuration**

Name: \*CEtls-COLCM9PUB ⓘ

Type: Neighbor

Hop count: 15 ⓘ

**H.323**

Mode: Off ⓘ

**SIP**

Mode: On ⓘ

Port: \*5061 ⓘ

Transport: TLS ⓘ

TLS verify mode: On ⓘ

Media encryption mode: Best effort ⓘ

ICE support: Off ⓘ

**Authentication**

Authentication policy: Treat as authenticated ⓘ

SIP authentication trust mode: Off ⓘ

**Location**

Peer 1 address: COLCM9PUB.coluc.com ⓘ SIP: Reachable: 10.48.55.96:5061

# ExpressWay – Mobile and Remote Access

## UC Server discovery

- Search Rule on ExpressWay C is automatically added

**Search rules** You are here: [Configuration](#) > [Dial plan](#) > Search rules

Priority	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	State	Actions
45	<a href="#">CEtcp-COLCM9PUB</a>	SIP	Any	No	Alias pattern match	Prefix	COLCM9PUB;transport=TCP	Leave	Stop	<a href="#">CEtcp-COLCM9PUB</a>	✓ Enabled	<a href="#">View</a>
45	<a href="#">CEtls-COLCM9PUB</a>	SIP	Any	No	Alias pattern match	Prefix	COLCM9PUB;transport=TLS	Leave	Stop	<a href="#">CEtls-COLCM9PUB</a>	✓ Enabled	<a href="#">View</a>
45	<a href="#">CEtcp-COLCM9SUB1</a>	SIP	Any	No	Alias pattern match	Prefix	COLCM9SUB1;transport=TCP	Leave	Stop	<a href="#">CEtcp-COLCM9SUB1</a>	✓ Enabled	<a href="#">View</a>
45	<a href="#">CEtls-COLCM9SUB1</a>	SIP	Any	No	Alias pattern match	Prefix	COLCM9SUB1;transport=TLS	Leave	Stop	<a href="#">CEtls-COLCM9SUB1</a>	✓ Enabled	<a href="#">View</a>
<input type="checkbox"/>	<a href="#">LocalZoneMatch</a>	Any	Any	No	Any alias				Continue	LocalZone	✓ Enabled	<a href="#">View/Edit</a>

Hide generated items

Search rules are applied in priority order, with 1 being the highest priority

# ExpressWay – Mobile and Remote Access

## UC Server discovery

- Search Rules on none-configurable

**Edit search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Edit search rule

**Configuration**

Rule name	<input type="text" value="*CEtcp-COLCM9PUB"/> <i>i</i>
Description	<input type="text" value="CE for UCM TCP COLCM9PUB"/> <i>i</i>
Priority	<input type="text" value="45"/> <i>i</i>
Protocol	<input type="text" value="SIP"/> <i>i</i>
Source	<input type="text" value="Any"/> <i>i</i>
Request must be authenticated	<input type="text" value="No"/> <i>i</i>
Mode	<input type="text" value="Alias pattern match"/> <i>i</i>
Pattern type	<input type="text" value="Prefix"/> <i>i</i>
Pattern string	<input type="text" value="*COLCM9PUB;transport=TCP"/> <i>i</i>
Pattern behavior	<input type="text" value="Leave"/> <i>i</i>
On successful match	<input type="text" value="Stop"/> <i>i</i>
Target	CEtcp-COLCM9PUB - Zone
State	<input type="text" value="Enabled"/> <i>i</i>



# DNS and Domain configuration

# Domain Configuration

## ExpressWay C – Domain Configuration

> Configurations > Domains

### Domains

You are here: [Configuration](#) > [Domains](#) > [Edit](#)

#### Configuration

Domain name

\* coluc.com



#### Supported services for this domain

SIP registrations and provisioning on Unified CM

On



IM and Presence services on Unified CM

On



Save

Delete

Cancel




# Domain Configuration

## ExpressWay C & E – DNS Configuration






- System > DNS

**DNS**

**DNS settings**

System host name	<input type="text" value="xwayc"/>	
Domain name	<input type="text" value="coluc.com"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

**Default DNS servers**

Address 1	<input type="text" value="10.48.83.51"/>	
Address 2	<input type="text"/>	
Address 3	<input type="text"/>	
Address 4	<input type="text"/>	
Address 5	<input type="text"/>	

# Collaboration Edge Service Record (SRV)

- For a Jabber client to be able to log in successfully with MRA, a specific collaboration edge SRV record must be created and accessible externally. When a Jabber client is initially started, it makes DNS SRV queries:
- **\_\_cisco-uds**: This SRV record is used in order to determine if a CUCM server is available.
- **\_\_cuplogin**: This SRV record is used in order to determine if an IM&P server is available.
- **\_\_collab-edge**: This SRV record is used in order to determine if MRA is available.



# Client Service Discovery

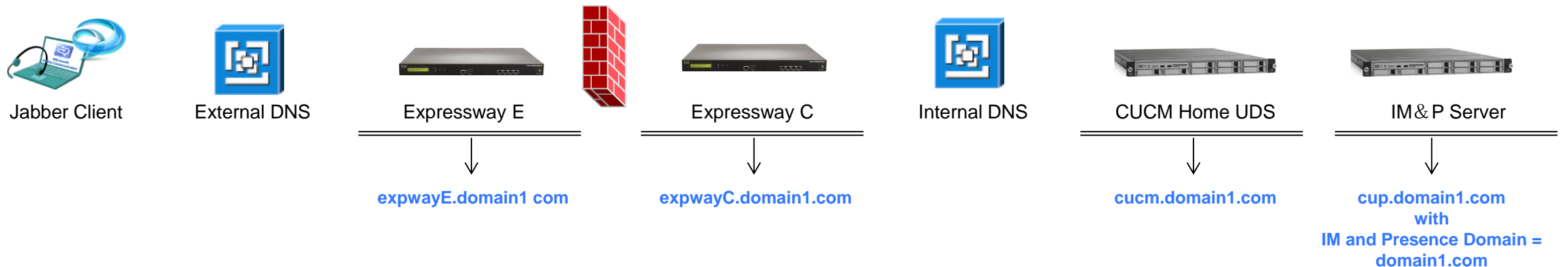
- Service discovery enables clients and endpoints to automatically detect and locate service.
- The client/endpoint does query DNS servers to retrieve service (SRV) records that provide the location of servers.
- Clients/endpoints outside the internal network must be able to resolve ‘\_collab-edge.\_tls.<domain>’ SRV record which must point to the ExpressWay E server.
- Clients/endpoints but also ExpressWay C must be able to resolve ‘\_cisco-uds.\_tcp.<domain>’ SRV record which must point to the CUCM cluster.
- The external DNS may not resolve ‘\_cisco-uds.\_tcp’ SRV records
- The internal DNS may not resolve ‘\_collab-edge.\_tls’ SRV records

# Client Service Discovery

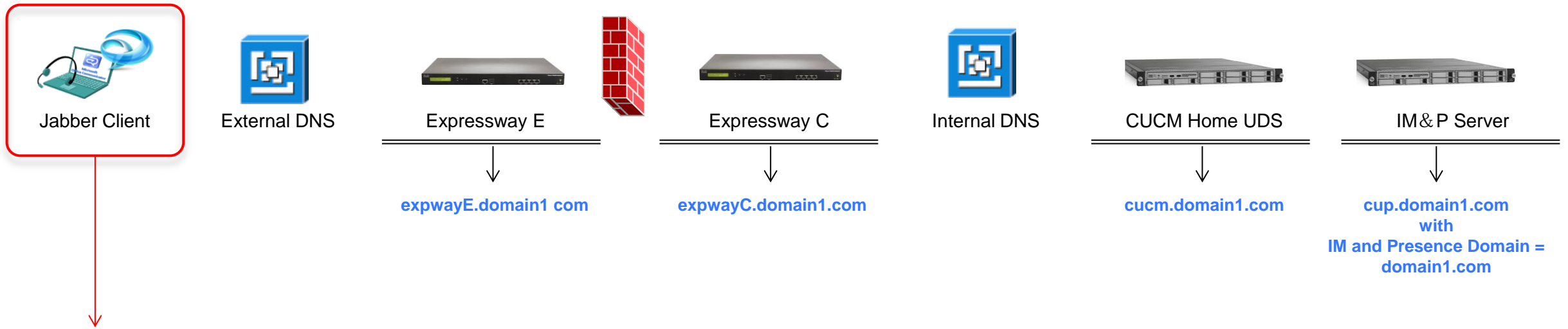
- If the Jabber client is started and **does not** receive an SRV answer for **\_cisco-uds** and **\_cuplogin** and **does** receive an answer for **\_collab-edge**, then it uses this answer to try to contact the Expressway-E listed in the SRV answer.
- The **\_collab-edge** SRV record should point to the Fully Qualified Domain Name (FQDN) of Expressway-E with port **8443**. If the **\_collab-edge** SRV is not created, or is not externally available, or if it is available, but port 8443 is not reachable, then the Jabber client fails to log in.

# ExpressWay Mobile and Remote Access Domain & DNS configuration

- Scenario
  - Flat domain structure
  - ExpressWay Servers : domain1.com
  - UC servers : domain1.com
  - IM&P domain : domain1.com



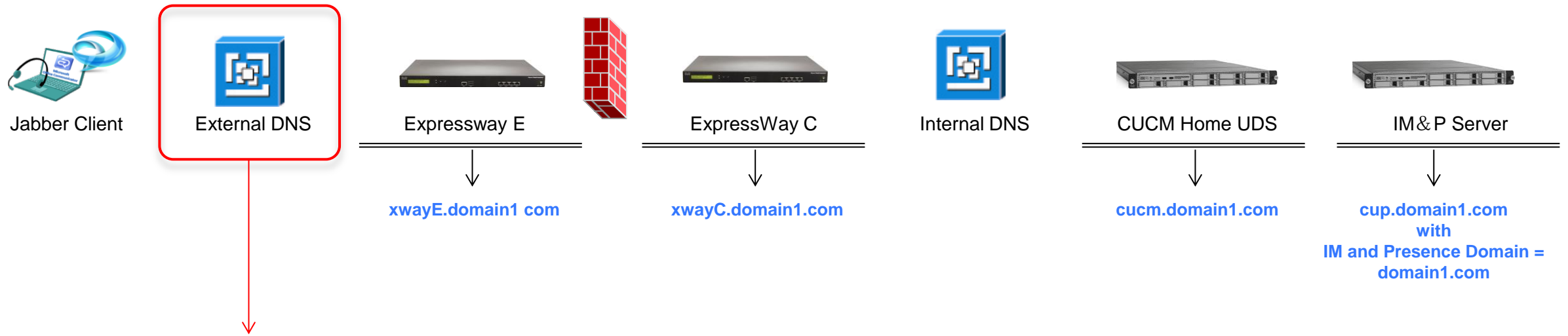
# ExpressWay Mobile and Remote Access Domain & DNS configuration



Question : How do I login?

Answer : With <userid>@domain1.com

# ExpressWay Mobile and Remote Access Domain & DNS configuration

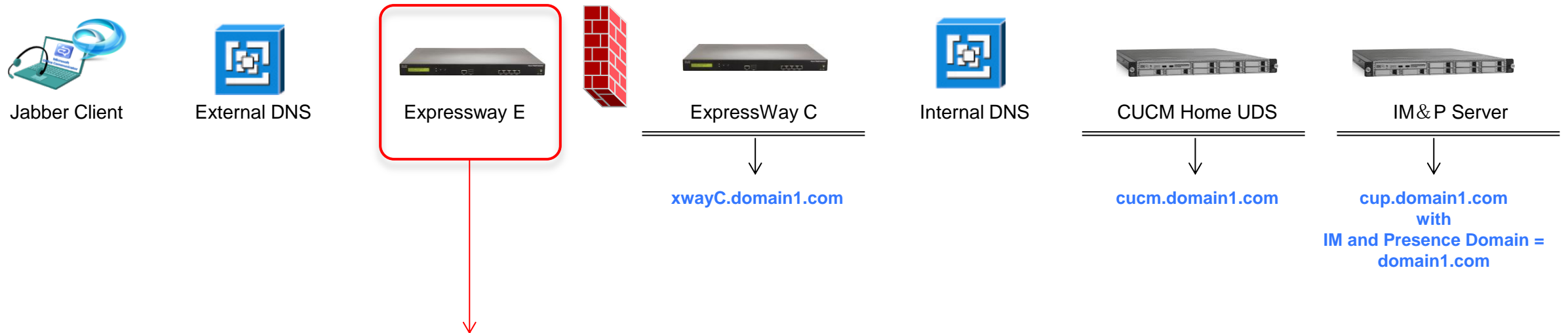


Question: How is my external DNS configured?

Answer:

Entry	Resolves to
SRV record ' <code>_collab-edge._tls.domain1.com</code> '	<code>xwayE.domain1.com</code> port 8443
A record ' <code>xwayE.domain1.com</code> '	External IP address ExpressWay E

# ExpressWay Mobile and Remote Access Domain & DNS configuration



Question: How is my ExpressWay E configured?

Answer:

> System > DNS >

- System host name 'xwayE'
- Domain name 'domain1.com'

# ExpressWay Mobile and Remote Access Domain & DNS configuration



Question: How is my ExpressWay C configured?

Answer:

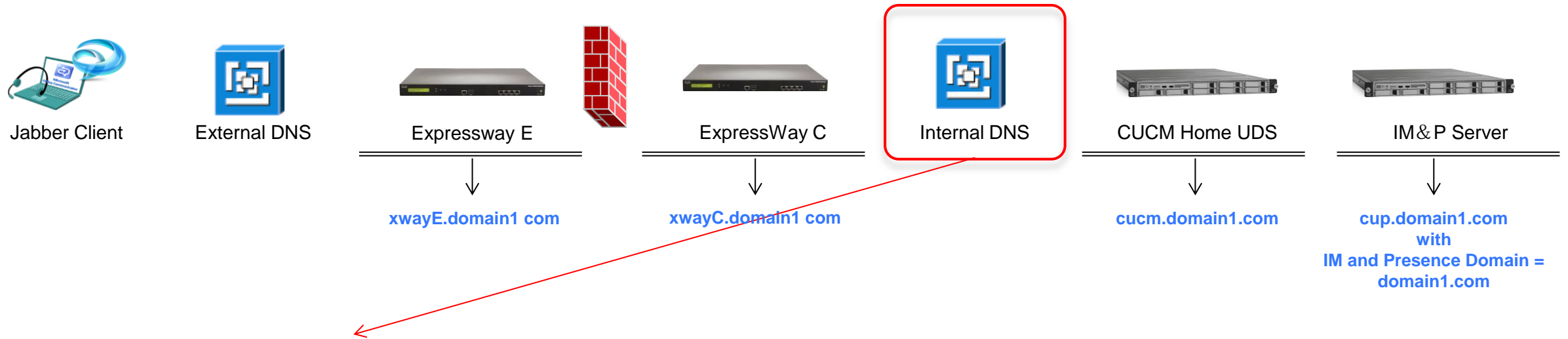
> System > DNS >

- System host name 'xwayC'
- Domain name 'domain1.com'

> Configuration > Domains >

- Domain 'domain1.com' enabled for 'UCM registrations' and 'IM and Presence'

# ExpressWay Mobile and Remote Access Domain & DNS configuration



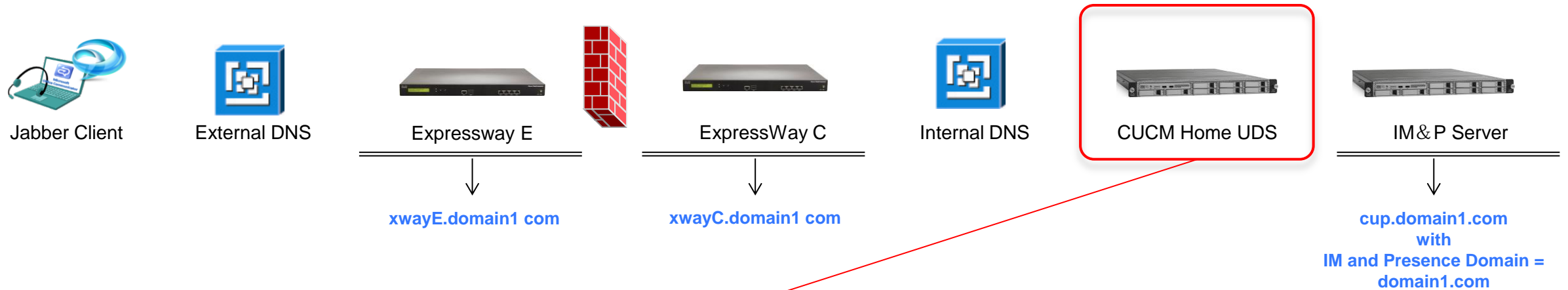
Question: How is my Internal DNS configured?

Answer:

Entry	Resolves to
SRV record ' <code>_cisco-uds._tcp.domain1.com</code> '	<code>cucm.domain1.com</code> port 8443
A record ' <code>cucm.domain1.com</code> '	IP address of CUCM
SRV record ' <code>_cuplogin._tcp.domain1.com</code> '	<code>cup.domain1.com</code> port 8443
A record ' <code>cup.domain1.com</code> '	IP address of CUP



# ExpressWay Mobile and Remote Access Domain & DNS configuration

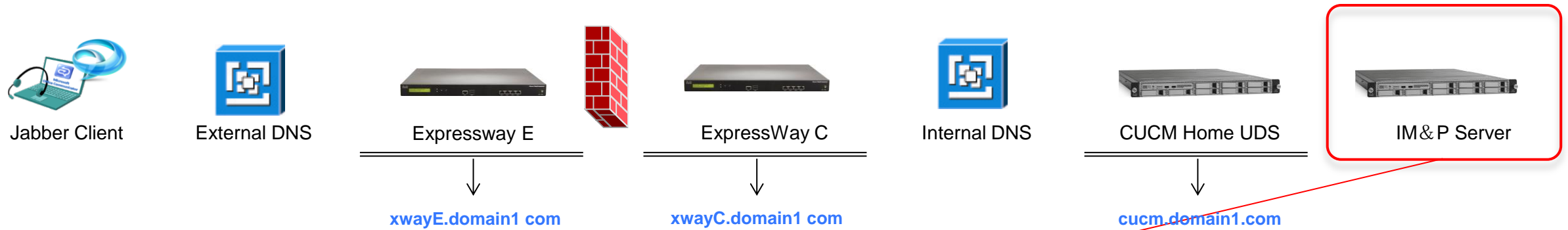


Question: How is my CUCM configured?

Answer:

- > CCMADMIN > System > Server
  - Server with hostname 'cucm'
- > CLI 'set network domain 'domain1.com'

# ExpressWay Mobile and Remote Access Domain & DNS configuration



Question: How is my CUP configured?

Answer:

> CUPAdmin > Clustertopology

- Node configuration with 'cup.domain1.com'
- IM and Presence Domain with 'domain1.com'(\*)

(\*) Only 1 is supported

# ExpressWay Mobile and Remote Access

## ExpressWay or UC Server Domain not configured

- ExpressWay or UC server domain not added or not enabled for Unified Communications
- Jabber login will fail – Cannot communicate with the server
- Diagnostic logs will show  
HTTPMSG:|GET  
[https://Y29sdWMuY29t/get\\_edge\\_config?service\\_name=\\_cisco-uds&service\\_name=\\_cuplogin](https://Y29sdWMuY29t/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin)  
HTTP/1.1Authorization: xxxxxHost: xwaye.coluc.com:8443  
Accept: \*/\*User-Agent: Jabber-Win-345  
  
HTTPMSG:|HTTP/1.1 **403 Forbidden**  
Date:  
Mon, 17 Mar 2014 16:07:20 GMT  
Connection: closeServer:  
CE\_EContent-Length: 0|

Decodes to 'coluc.com'



# ExpressWay Mobile and Remote Access IM&P Domain not configured (UC Domain)

- IM&P domain not added or not enabled for IM&P
- Jabber login will fail – Cannot communicate with the server
- Diagnostic logs will show

```
xway XCP_JABBERD[12144]: UTCTime="2014-03-14 14:30:25,310"  
ThreadID="140582990952192" Module="Jabber" Level="INFO " CodeLocation="deliver.c:1492"  
Detail="bouncing a packet to 'domain3.com' from 'cm-1_jsmcp-1.xwaye-domain1.com'"
```

```
xway XCP_CM[12513]: UTCTime="2014-03-14 14:30:25,310" ThreadID="140004551300864"  
Module="cm-1.xwaye-domain1.com" Level="INFO " CodeLocation="SASLManager.cpp:198"  
Detail="Failed to query auth component for SASL mechanisms"
```



# Serviceability ExpressWay

# ExpressWay C “Unified Communications” status

- Status > Unified Communications

**Unified Communications** You are here: [Status](#) > [Unified Communications](#)

**Unified Communications (last updated: 18:23:24 UTC)**

Unified Communications status	Enabled
Unified Communications services	Active
IM and Presence servers	1
Unified CM servers	2

**Activity**

Current provisioned sessions	2
Total provisioning requests since last restart	2
Total provisioned sessions since last restart	2
Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0

**Domains**

Name	Services	Associated zones
coluc.com	Unified CM registrations, IM and Presence	TraversalZone

**Zones**

Name	SIP status
<a href="#">TraversalZone</a>	Active

**Advanced status information**

- [View provisioning sessions](#)
- [View ssh tunnel status](#)

# ExpressWay C “Unified Communications” status

- Unified Communications > View provisioned sessions

## Unified Communications proxy requests

You are here: [Status](#) > [Unified Communications](#) > Unified Communications proxy requests

Records: 5

Page 1 of 1

Username	Device	User agent	Unified CM server	Expire time
ewayj	10.10.1.7	Jabber-Win-293	colcm9pub	2014-03-26 02:22:48
ewayj	10.10.1.7	Jabber-Win-969	colcm9pub	2014-03-26 00:44:10
ewayj	10.10.1.7	Jabber-Win-101	colcm9pub	2014-03-26 00:45:50
ewayj	10.10.1.7	Jabber-Win-293	colcm9pub	2014-03-26 02:22:49
ewayj	10.10.1.7	Jabber-Win-101	colcm9pub	2014-03-26 00:45:49

### Related tasks

[View Unified CM servers](#)

# ExpressWay E – “Unified Communications” status

- Status > Unified Communications

**Unified Communications** You are here: [Status](#) > Unified Communications

**Unified Communications (last updated: 18:24:41 UTC)**

Unified Communications status	Enabled
Unified Communications services	Active

**Activity**

Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0

**Domains**

Name	Services	Associated zones
coluc.com	Unified CM registrations, IM and Presence	TraversalZone

**Zones**

Name	SIP status
<a href="#">TraversalZone</a> (xwayc.coluc.com)	Active

**Advanced status information**

[View ssh tunnel status](#)



# ExpressWay C – “Call Status”

- Status > Calls > Calls (active) or History

**Call status** You are here: [Status](#) > [Calls](#) > [Calls](#)

Records: 1 Page 1 of 1

Start time ^	Duration	Source	Destination	Type	Protocol	Peer	Actions
<input type="checkbox"/> <a href="#">2014-03-25 18:27:08</a>	1 minute 56 seconds	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	Traversal	Multiple components	This system	<a href="#">View</a>

[Disconnect](#) | [Select all](#) | [Unselect all](#)

**Call status** You are here: [Status](#) > [Calls](#) > [Calls](#) > [View](#)

Status	
Status	Connected
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Box-unique call serial number	4b3abe17-358f-4f57-a757-ff9eeed39ee1
Source alias	sip:5000@COLCM9PUB
Destination alias	sip:9011@COLCM9PUB
Start time	2014-03-25 18:27:08
Duration	2 minutes 31 seconds

Call components				
Local call serial number	Source alias	Destination alias	Protocol	Type
<a href="#">a5988187-374e-424c-80fc-a7df8cf101d3</a>	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway
<a href="#">daa60af9-a970-483a-99fc-f90f4dc21d19</a>	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Encryption B2BUA
<a href="#">9a4db343-a8fd-43ad-9476-b93af9fc635b</a>	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway

[Disconnect](#)

# ExpressWay C – Traversal Call

## Call details

You are here: [Status](#) > [Calls](#) > [Calls](#) > Call details

Call information	
State	Connected
Start time	2014-03-25 18:27:08
Duration	5 minutes 39 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	a5988187-374e-424c-80fc-a7df8cf101d3
Type	Video
Bandwidth	
Requested	4000 kbps
Allocated	64 kbps
Route	TraversalZone -> Zone001ToTraversalSZ -> TraversalSubZone -> Zone004ToTraversalSZ -> CEts-COLCM9PUB
Leg 1	
Bandwidth node	TraversalZone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.48.55.99:7001
Transport	TLS
Encryption type	None
Leg 2	
Bandwidth node	
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	Not set
Transport	SIP Transport Protocol Undefined
Leg 3	
Bandwidth node	CEts-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.96:5061
Transport	TLS
Leg 4	
Bandwidth node	CEts-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.98:5071
Transport	TLS
Encryption type	AES

Session 1	
Status	Searching
Media routed	False
Call routed	False
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	0 kbps
Bandwidth requested	0 kbps
Session 2	
Status	Replaced
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 3
Bandwidth allocated	0 kbps
Bandwidth requested	0 kbps
Session 3	
Status	Connected
Media routed	False
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 4
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	TraversalZone -> Zone001ToTraversalSZ -> TraversalSubZone -> Zone004ToTraversalSZ -> CEts-COLCM9PUB

- ExpressWay C  
B2BUA Call

### B2BUA calls

Call Information	
State	Active
Start time	2014-03-25 18:27:08
Duration	4 minutes 50 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Box call serial number	4b3abe17-358f-4f57-a757-ff9eeed39ee1

Route	
Route	Edge->Edge
Source	sip:5000@COLCM9PUB
Destination	sip:9011@COLCM9PUB

#### Related tasks

- [View summary of this call](#)
- [View media statistics for this call component](#)
- [View all events associated with this call](#)

# ExpressWay C – CUCM Call

## Call details

You are here: [Status](#) > [Calls](#) > [Calls](#) > [Call details](#)

### Call information

State	Connected
Start time	2014-03-25 18:27:08
Duration	7 minutes 16 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	9a4db343-a8fd-43ad-9476-b93af9fc635b
Type	Video

### Leg 1

Bandwidth node	Default zone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.48.55.98:5073
Transport	TLS
Encryption type	None

### Leg 2

Bandwidth node	CEtIs-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.96:5061
Transport	TLS
Encryption type	None

### Session 1

Status	Connected
Media routed	False
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2

# ExpressWay E – “Call Status”

## Call status

You are here: [Status](#) ▶ [Calls](#) ▶ [Calls](#)

Records: 1

Page 1 of 1

	Start time ▲	Duration	Source	Destination	Type	Protocol	Peer	Actions
<input type="checkbox"/>	<a href="#">2014-03-25 18:27:08</a>	9 minutes 26 seconds	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	Traversal	SIP <-> SIP	This system	<a href="#">View</a>

Disconnect

Select all

Unselect all

## Call status

You are here: [Status](#) ▶ [Calls](#) ▶ [Calls](#) ▶

### Status

Status	Connected
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Box-unique call serial number	3012e784-b45d-4a9a-b2f0-c4d1988fc5d1
Source alias	sip:5000@COLCM9PUB
Destination alias	sip:9011@COLCM9PUB
Start time	2014-03-25 18:27:08
Duration	9 minutes 54 seconds

### Call components

Local call serial number	Source alias	Destination alias	Protocol	Type
<a href="#">a198d507-6990-4fed-ab96-87d545bfc3ee</a>	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway

Disconnect

- ExpressWay E Inbound Call

**Call details** You are here: [Status](#) > [Calls](#) > [Calls](#) > [Call details](#)

Call Information	
State	Connected
Start time	2014-03-25 18:27:08
Duration	12 minutes 23 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	a198d507-6990-4fed-ab96-87d545bfc3ee
Type	Audio

Bandwidth	
Requested	4000 kbps
Allocated	64 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone

Leg 1	
Bandwidth node	CollaborationEdgeZone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.10.1.7:58999
Transport	TLS
Encryption type	AES

Session 1	
Status	Connected
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone

Leg 2	
Bandwidth node	TraversalZone
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.98:25742
Transport	TLS
Encryption type	AES

**Related tasks**

- [View summary of this call](#)
- [View media statistics for this call component](#)
- [View search details for this call component](#)
- [View all events associated with this call](#)

## ■ Inbound Call Media Statistics

**Call media** You are here: [Status](#) > [Calls](#) > [Calls](#) > [Call media](#)

Session Information	
Status	Connected
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone

Channel 1	
Type	Audio
Protocol	PCMU
Rate	70400 bps
Packets forwarded	33938
Keepalives	66
Errors	0
Duplicate packets	0
Lost packets	0
Out of order packets	0
Jitter	0 ms
From	sip:9011@COLCM9PUB

Channel 2	
Type	Audio
Protocol	PCMU
Rate	70635 bps
Packets forwarded	34096
Keepalives	68
Errors	0
Duplicate packets	0
Lost packets	0
Out of order packets	0
Jitter	0 ms
From	sip:5000@COLCM9PUB

# ExpressWay Tools

- Maintenance > Tools > Network Utilities

Ping

DNS lookup (also flush dns cache from DNS configuration)

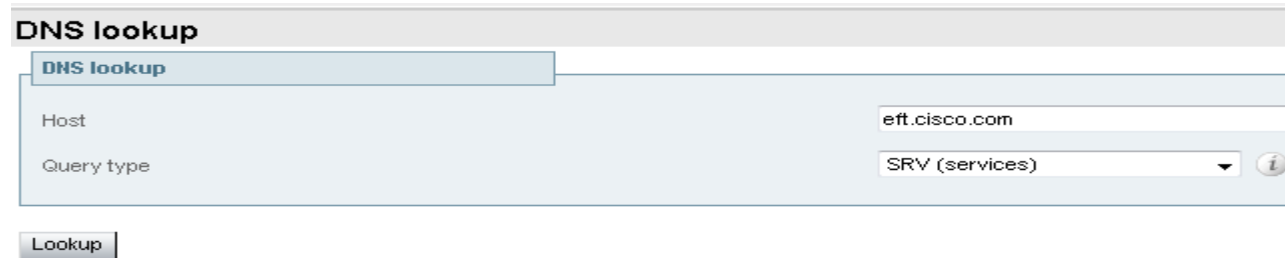
TraceRoute

TracePath



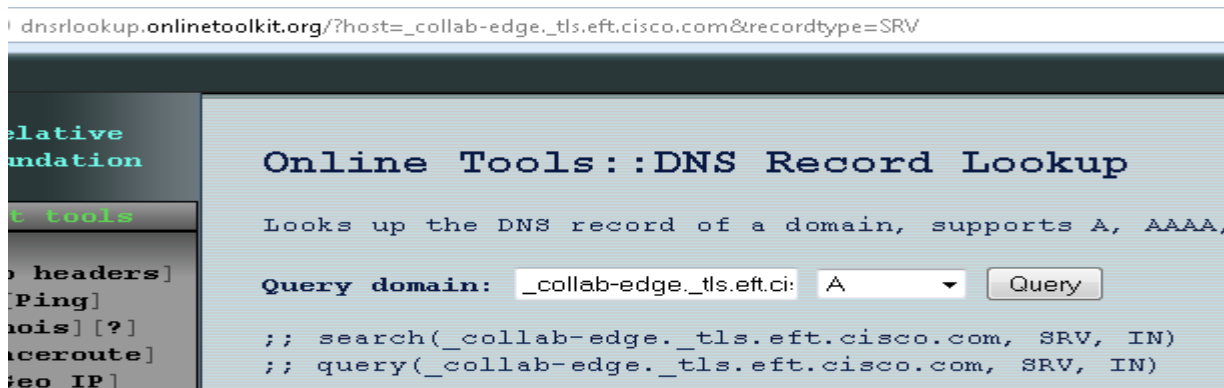
# DNS Lookup

- > Maintenance > Tools > Network Utilities > DNS Lookup (for internal DNS)



The screenshot shows a web-based interface for a DNS lookup tool. At the top, there is a header "DNS lookup". Below it, there is a sub-header "DNS lookup" in a light blue box. The main area contains two input fields: "Host" with the value "eft.cisco.com" and "Query type" with a dropdown menu set to "SRV (services)". There is an information icon to the right of the dropdown. Below the input fields is a "Lookup" button.

- Online Tools (for external) e.g <http://dnssrlookup.onlinetoolkit.org/>



The screenshot shows a web browser window with the URL `dnssrlookup.onlinetoolkit.org/?host=_collab-edge_tls.eft.cisco.com&recordtype=SRV`. The page title is "Online Tools::DNS Record Lookup". The main content area has a description: "Looks up the DNS record of a domain, supports A, AAAA,". Below this, there is a "Query domain:" label, a dropdown menu with "A" selected, and a "Query" button. At the bottom, there is a pre-formatted text area containing the following commands:  



```
;; search(_collab-edge_tls.eft.cisco.com, SRV, IN)
;; query(_collab-edge_tls.eft.cisco.com, SRV, IN)
```

# ExpressWay Diagnostic Logs

- Maintenance > Diagnostics > Diagnostic Logging

**Diagnostic logging** You are here: [Maintenance](#) > [Diagnostics](#) > Diagnostic logging

**Logging status**

Started logging at	Tuesday 25th of March 2014 11:35:14 PM
Stopped logging at	Tuesday 25th of March 2014 11:36:12 PM
Marker	<input type="text"/> 
	<input type="button" value="Add marker"/>
Take tcpdump while logging	<input type="checkbox"/> 

(When using dual NIC will take TCPdump on internal interface, when required from external need to SSH into ExpressWay (root) and run e.g “tcpdump -s 0 -w -i eth1 /tmp/trace-1.pcap” and use wincp to transfer)

# Jabber Registration Walk Through

# Jabber pre-requirements

- Jabber 9.6 (Win/iOS) requires configuration key in **jabber-config.xml** to enable Mobile Remote Access:

```
</Policies>  
  <RemoteAccess>ON</RemoteAccess>  
</Policies>
```

- For local testing purposes, user can set the RemoteAccess configuration key on their device editing **jabberLocalConfig.xml** (J4Win)

```
<Jabber>  
  <userConfig name="remoteaccess" value="ON"/>  
</Jabber>
```

→ In the officially supported version of Jabber (9.7)  
Mobile and Remote Access will be enabled by default

# Jabber URL transform

- Jabber transforms original Url: <http://colcm9pub:6970/CSFxwayj.cnf.xml>
- Base Url with appended Edge domain: coluc.com/
- Base Url with appended protocol: coluc.com/http/
- Base Url with appended host: coluc.com/http/colcm9pub
- Base Url before encoding: **coluc.com/http/colcm9pub/6970**
- Encoded Base64 Url: **Y29sdWMuY29tL2h0dHAvY29sY205cHVlLzY5NzA=**
- Transformed Url:

**https://xwaye.coluc.com:8443/Y29sdWMuY29tL2h0dHAvY29sY205cHVlLzY5NzA=/CSFxwayj.cnf.xml**

# Jabber URL Transfer

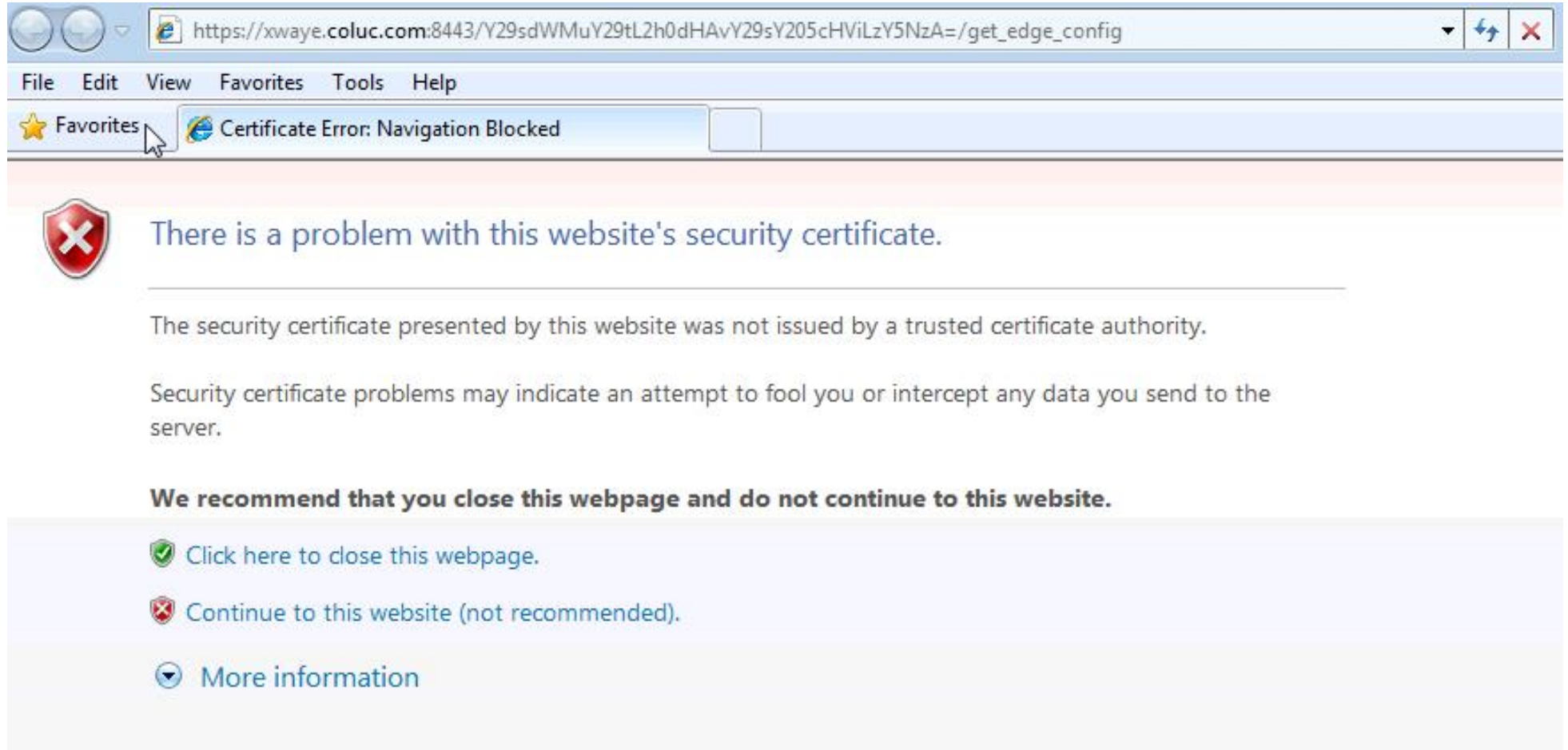
- A good way to verify that the basic MRA components are in place is to run the first HTTP request Jabber would do.
- To do this verification, open a browser and enter the following URL to verify that the HTTP Reverse proxy is working, and that the ExpressWay-C can discover the DNS.

[https://xwaye.coluc.com:8443/Y29sdWMuY29tL2h0dHAvY29sY205cHViLzY5NzA=/get\\_edge\\_config](https://xwaye.coluc.com:8443/Y29sdWMuY29tL2h0dHAvY29sY205cHViLzY5NzA=/get_edge_config)

- Use a CUCM User credentials when prompted by the browser
- Use <http://www.base64decode.org/> to encode/decode

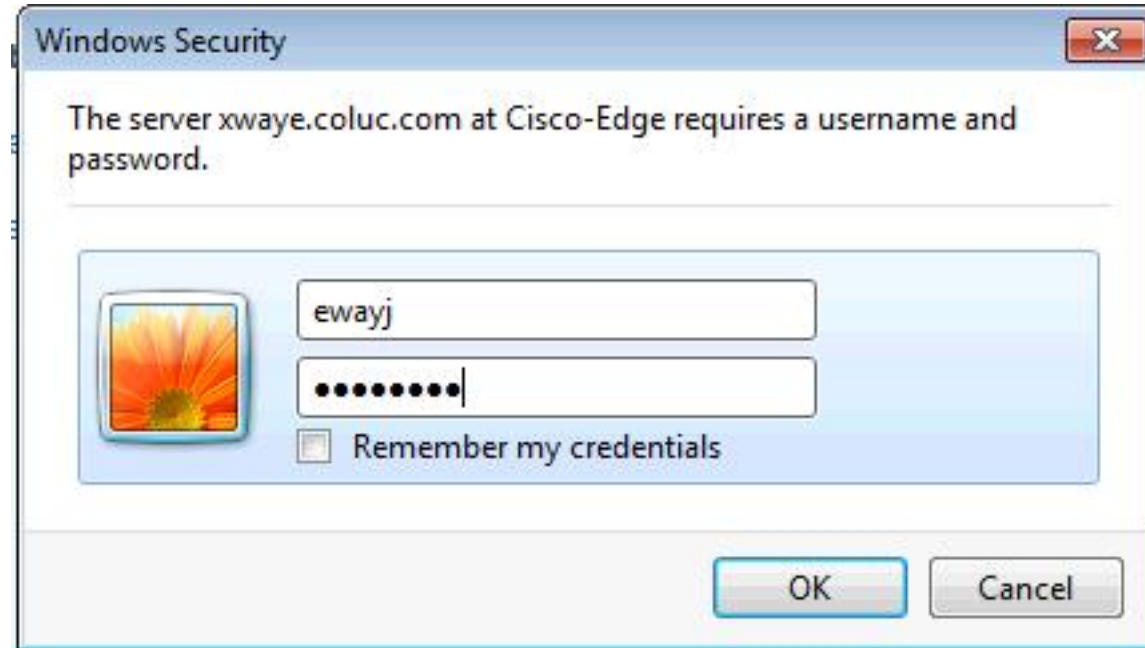
# Jabber URL Transform

- Expressway E certificate not trusted (Jabber client will prompt same)



# Jabber URL Transform

- Provide CCM user credentials





# Jabber URL Transform

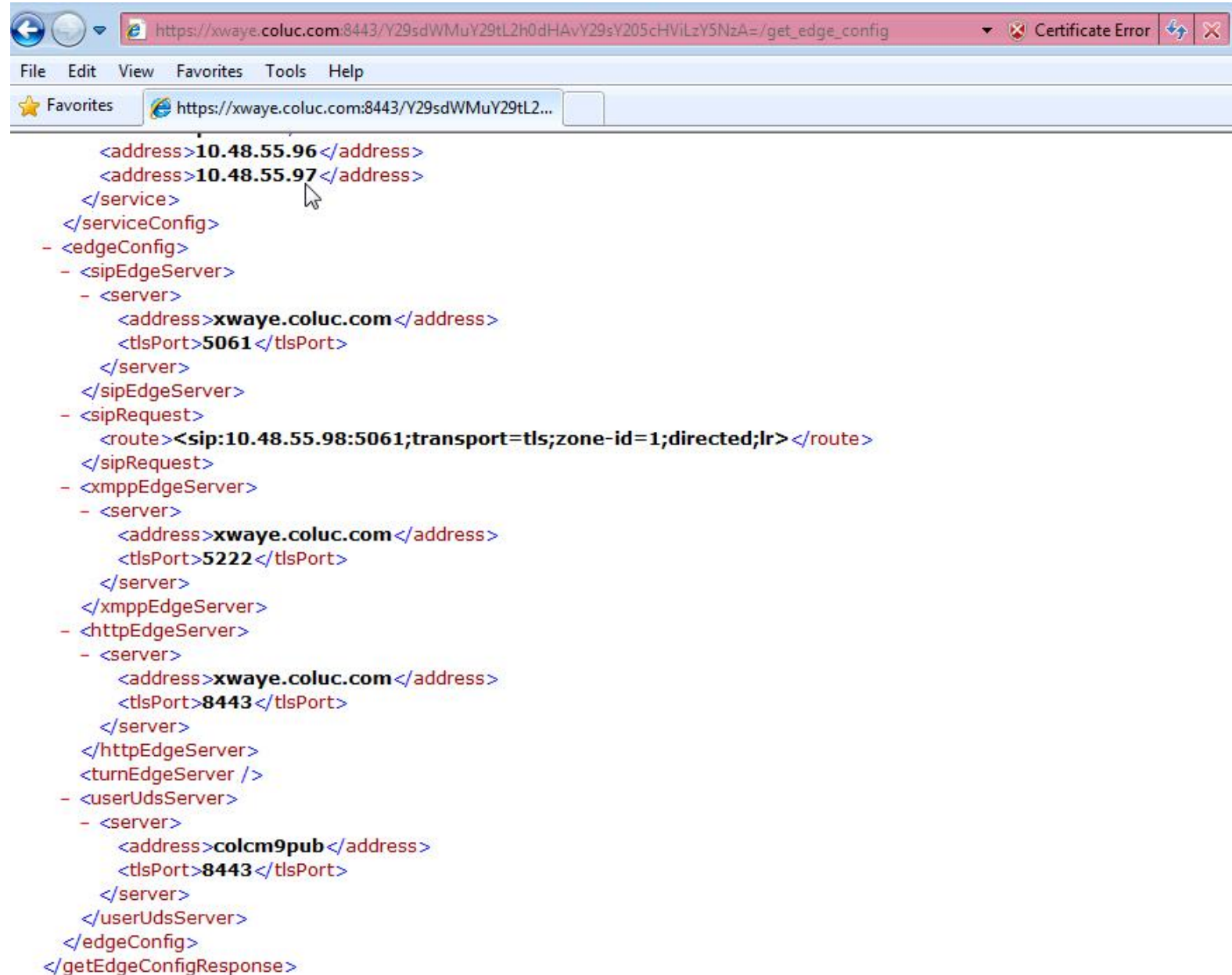
- Service Config



```
<?xml version="1.0" encoding="UTF-8" ?>
- <getEdgeConfigResponse version="1.0">
- <serviceConfig>
- <service>
  <name>_cisco-phone-tftp</name>
  - <server>
    <priority>0</priority>
    <weight>0</weight>
    <port>8443</port>
    <address>colcm9pub.coluc.com</address>
  </server>
</service>
- <service>
  <name>_cuplogin</name>
  <error>NameError</error>
</service>
- <service>
  <name>_cisco-uds</name>
  - <server>
    <priority>0</priority>
    <weight>0</weight>
    <port>8443</port>
    <address>colcm9pub.coluc.com</address>
  </server>
</service>
- <service>
  <name>tftpServer</name>
  <address>10.48.55.96</address>
  <address>10.48.55.97</address>
</service>
</serviceConfig>
```

# Jabber URL Transform

- Edge Configuration



```
<address>10.48.55.96</address>
<address>10.48.55.97</address>
</service>
</serviceConfig>
- <edgeConfig>
- <sipEdgeServer>
- <server>
  <address>xwaye.coluc.com</address>
  <tlsPort>5061</tlsPort>
</server>
</sipEdgeServer>
- <sipRequest>
  <route><sip:10.48.55.98:5061;transport=tls;zone-id=1;directed;lr></route>
</sipRequest>
- <xmppEdgeServer>
- <server>
  <address>xwaye.coluc.com</address>
  <tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
- <httpEdgeServer>
- <server>
  <address>xwaye.coluc.com</address>
  <tlsPort>8443</tlsPort>
</server>
</httpEdgeServer>
<turnEdgeServer />
- <userUdsServer>
- <server>
  <address>colcm9pub</address>
  <tlsPort>8443</tlsPort>
</server>
</userUdsServer>
</edgeConfig>
</getEdgeConfigResponse>
```

# Common Issue 1

## Softphone is Not Able to Register, SIP/2.0 405 Method Not Allowed

A diagnostic log from Expressway-C shows a **SIP/2.0 405 Method Not Allowed** message in response to the Registration request sent by the Jabber client. This is likely due to an existing Session Initiation Protocol (SIP) trunk between Expressway-C and CUCM using port 5060/5061.

### SIP/2.0 405 Method Not Allowed

```
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

In order to correct this issue, change the SIP port on the SIP Trunk Security Profile that is applied to the existing SIP trunk configured in CUCM and the Expressway-C neighbor zone for CUCM to a different port such as 5065. This is explained further in the [MRA Deployment Guide](#) on Page 39.

## Configuration Summary

### CUCM:

- 1.Create a new SIP Trunk security profile with a listening port other than 5060 (5065).
- 2.Create a SIP Trunk associated to the SIP Trunk Security Profile and destination set to the Expressway-C IP address, port 5060.

### Expressway-C:

- 1.Create a neighbor zone to CUCM(s) with a target port other than 5060 (5065) to match the CUCM configuration.
- 2.In Expressway-C **Settings > Protocols > SIP**, make sure Expressway-C still listens on 5060 for SIP.

# Common Issue 2

## Unable to Log In Because of an Existing WebEx Connect Subscription

Jabber for Windows logs show this:

```
2014-11-22 19:55:39,122 INFO [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://loginp.webexconnect.com;
Url: http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com';;2014-11-22
19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determinelsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]
success: [true] configStoreName: [LocalFileConfigStore]
```

The login attempts are directed to WebEx Connect.

For a permanent resolution, you must contact [WebEx](#) in order to have the site decommissioned.

## Workaround:

In the short-term, you can utilize one of these two options to exclude it from the lookup.

- Add this parameter to the jabber-config.xml. Then upload the jabber-config.xml file to the TFTP server on CUCM. It requires that the client logs in internally first.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

- From an application perspective, run this: **msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED\_SERVICES=WEBEX**

# Jabber Registration – Walk Trough

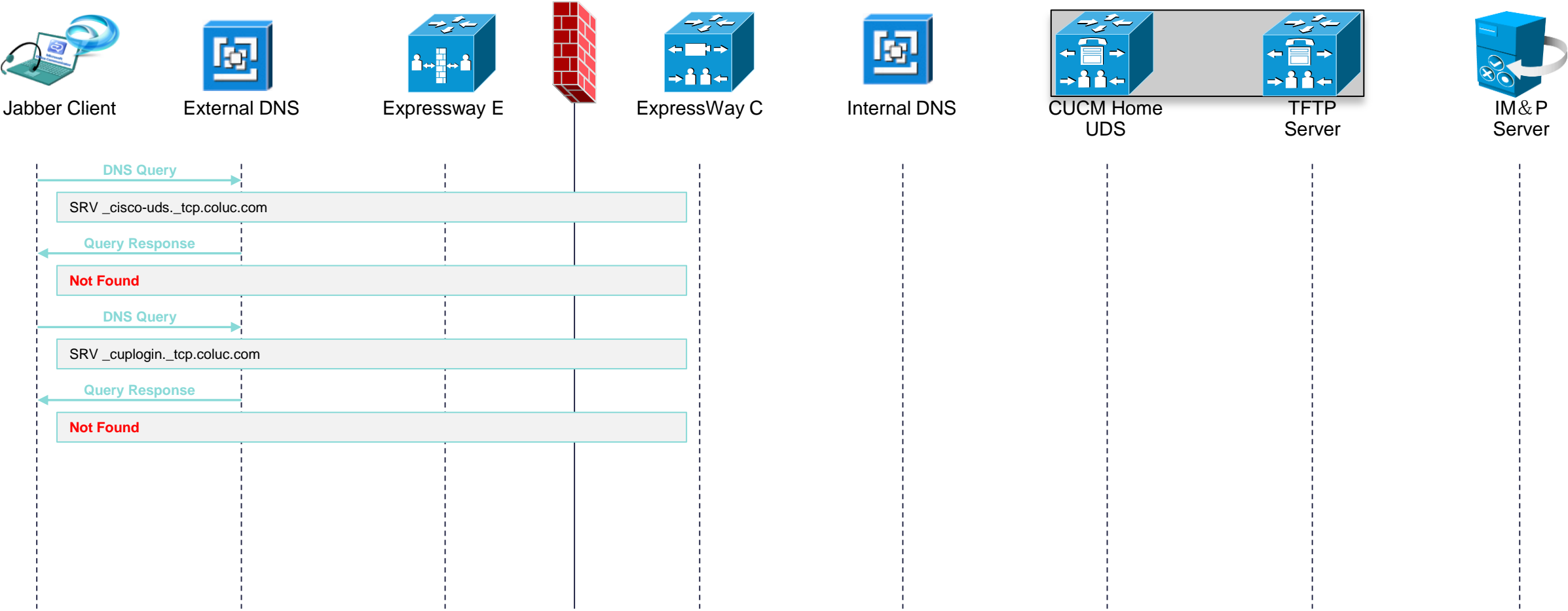
- Register Jabber client on UCM via MRA  
Expected signaling flow for Jabber Client logon and registration on simple IM&P based deployment



Jabber login with  
xwayj@coluc.com

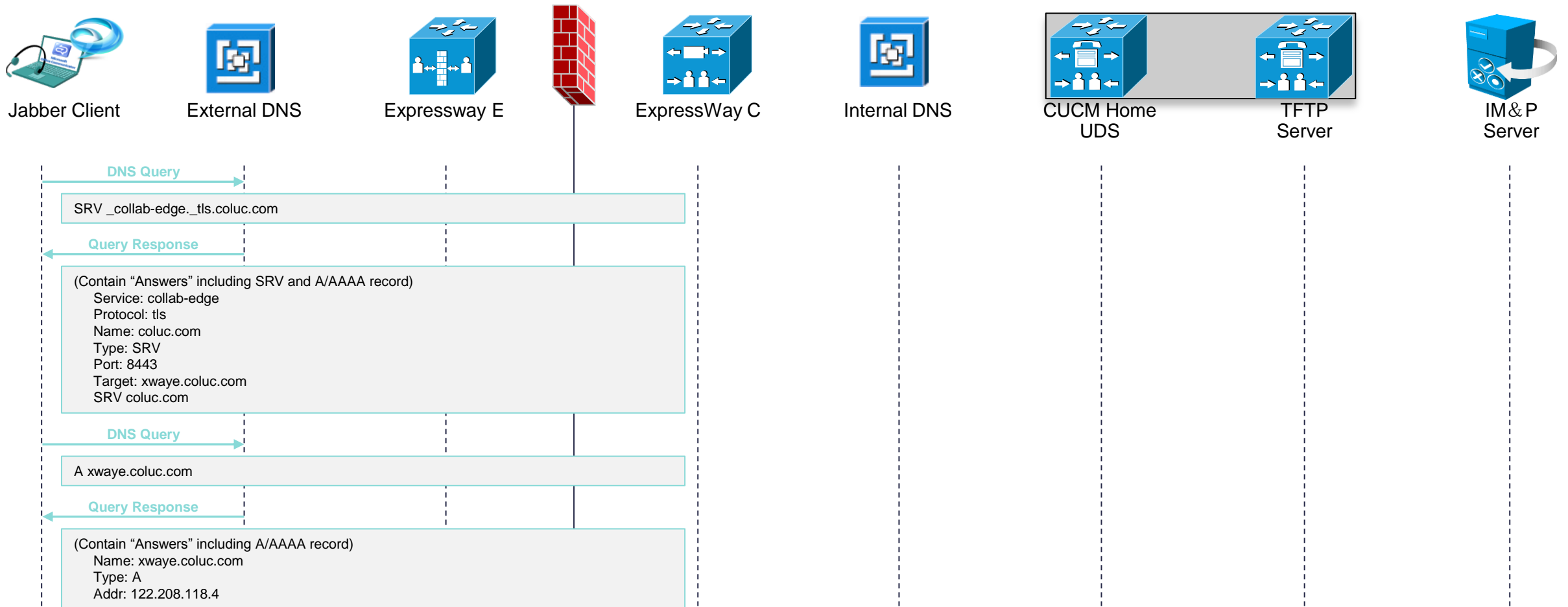
# Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



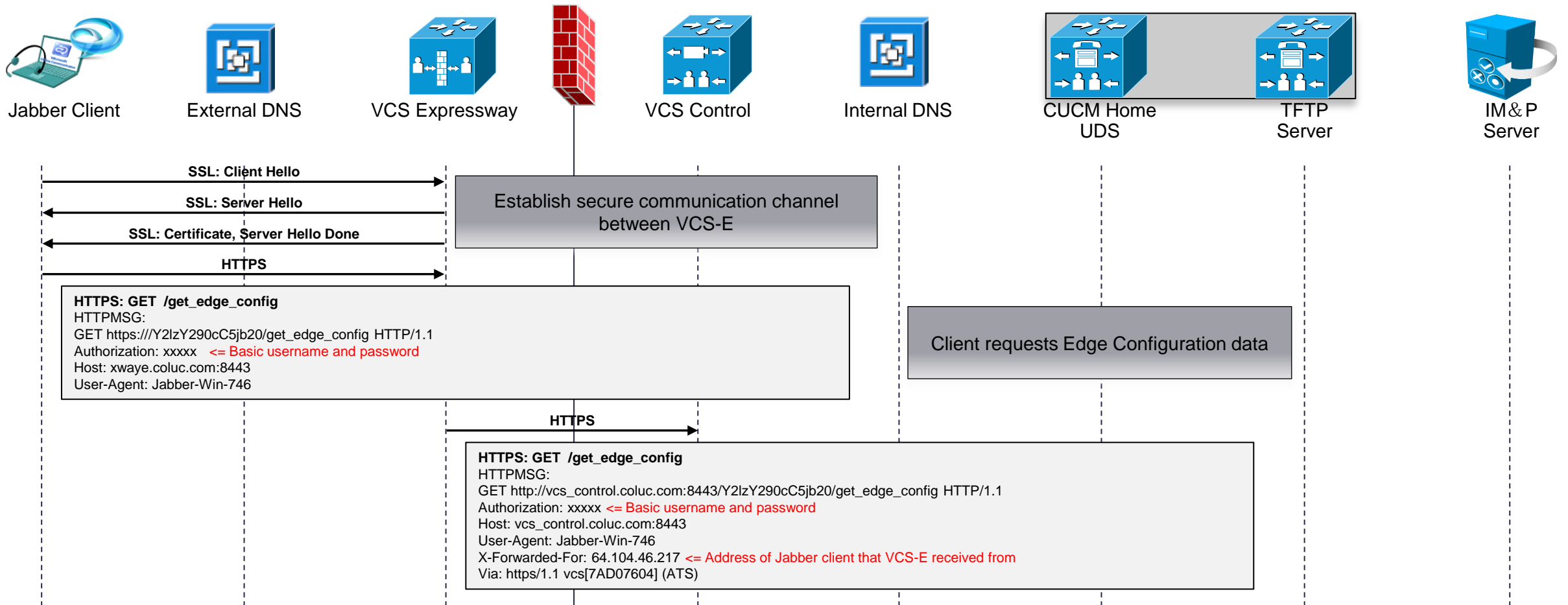
# Jabber Registration - Walk Through

- Register Jabber client on UCM via MRA



# Jabber Registration - Walk Trough

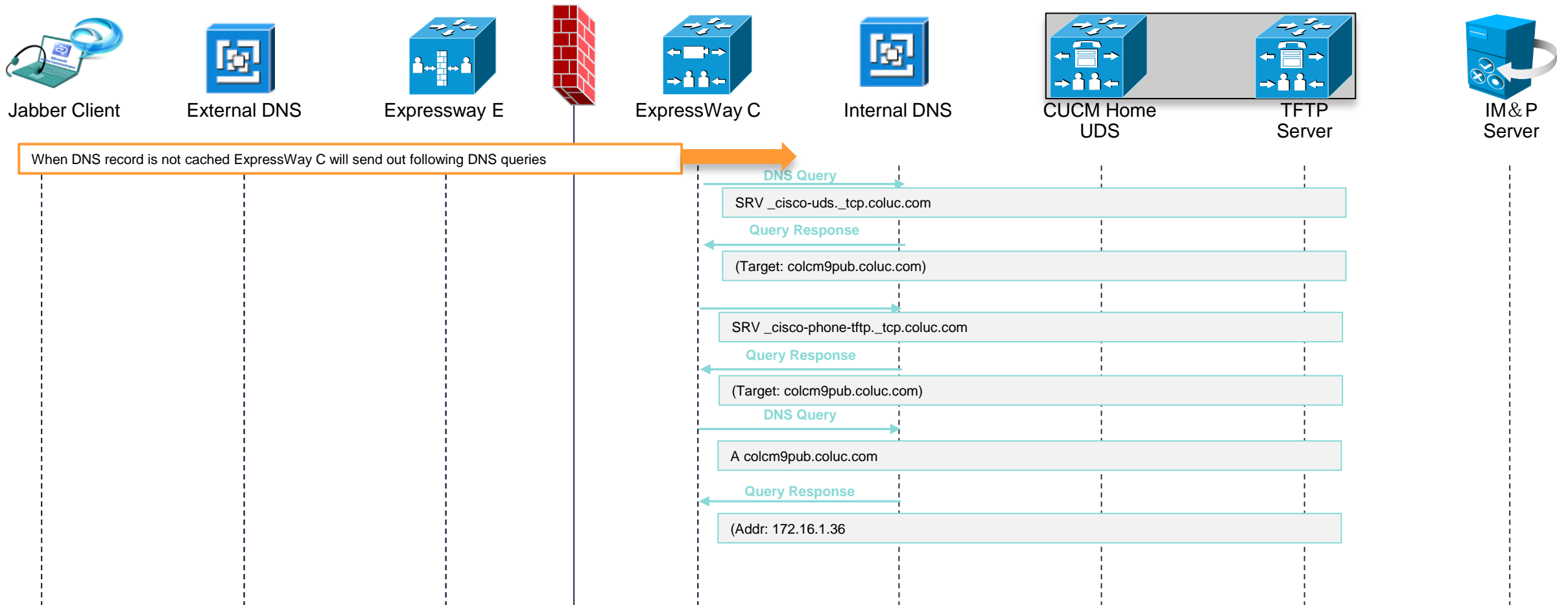
- Register Jabber client on UCM via MRA





# Jabber Registration - Walk Trough

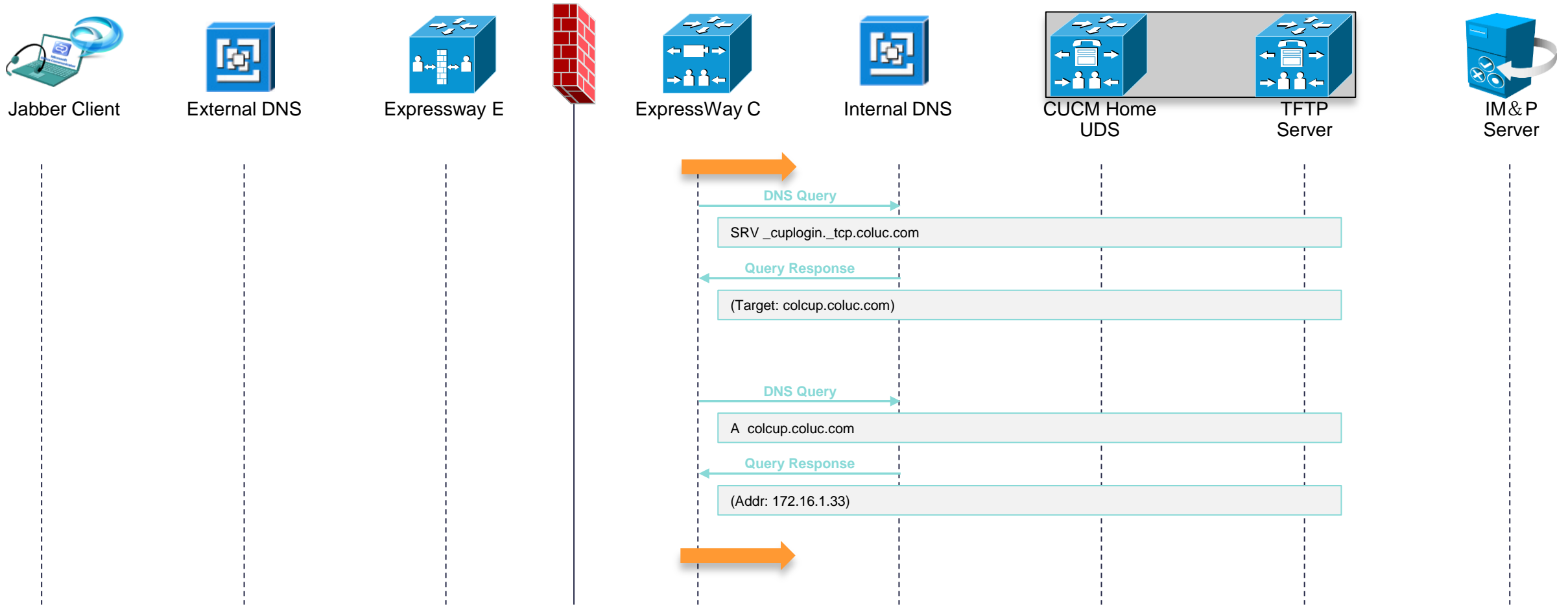
- Register Jabber client on UCM via MRA



# Mobile and Remote Access

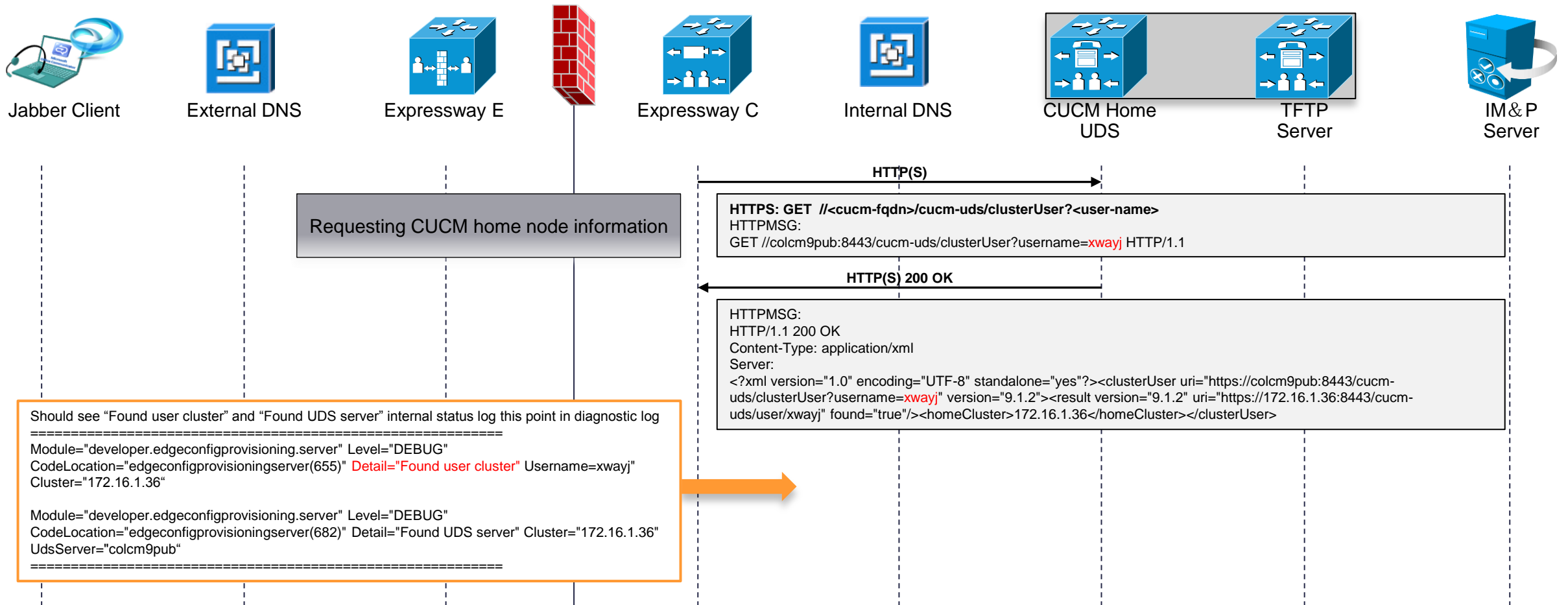
## - Jabber client connect through MRA

- Register Jabber client on UCM via MRA



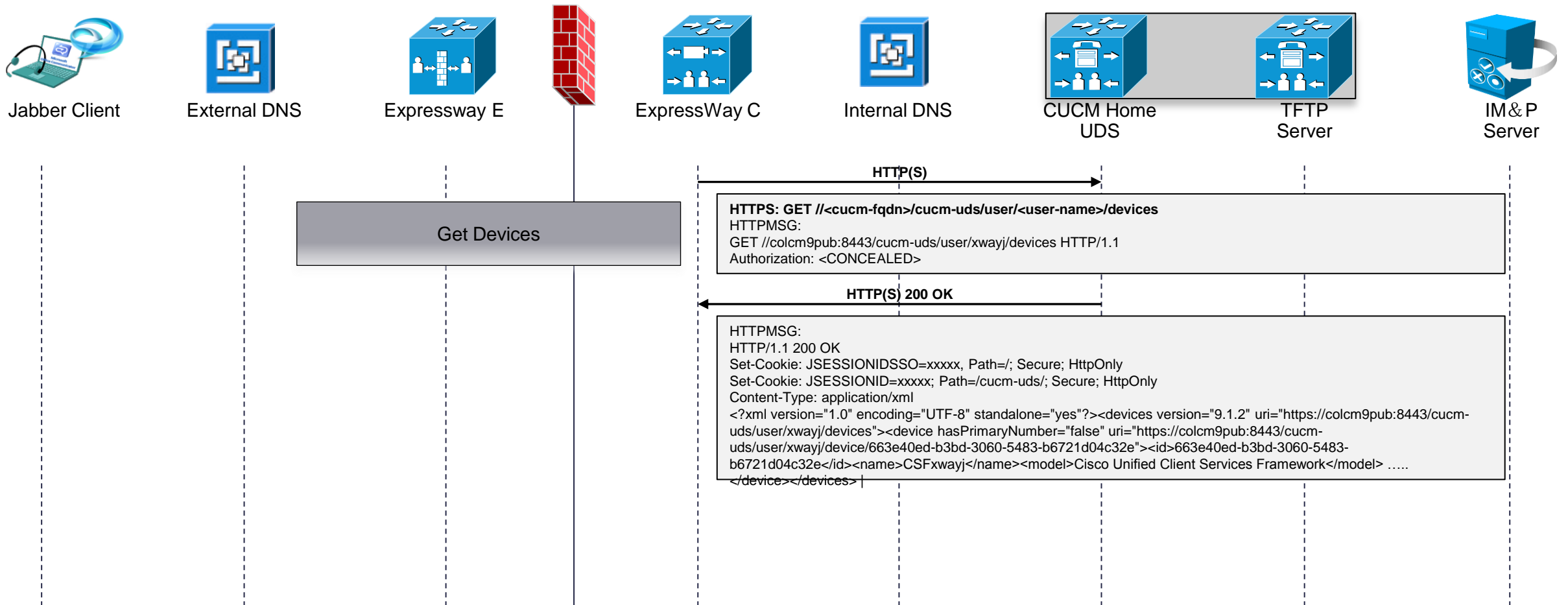
# Jabber Registration - Walk Trough

- Register Jabber client on UCM via MRA



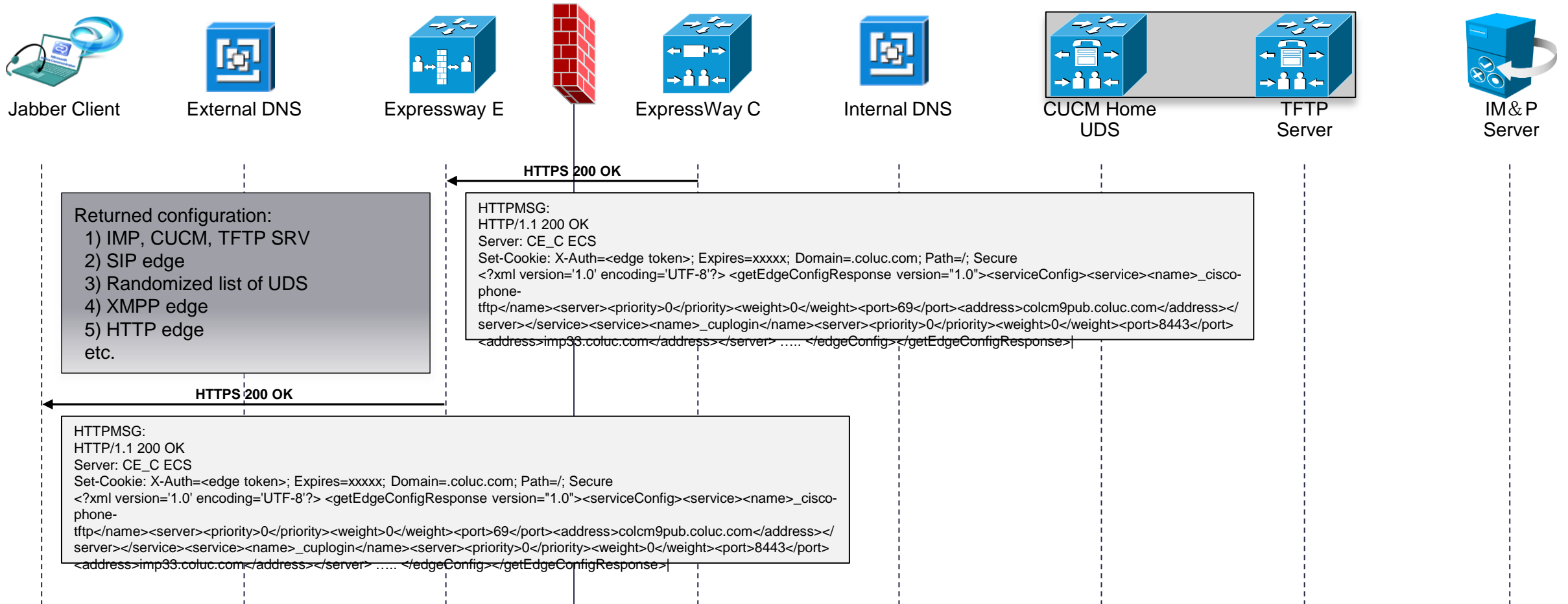
# Jabber Registration - Walk Trough

- Register Jabber client on UCM via MRA



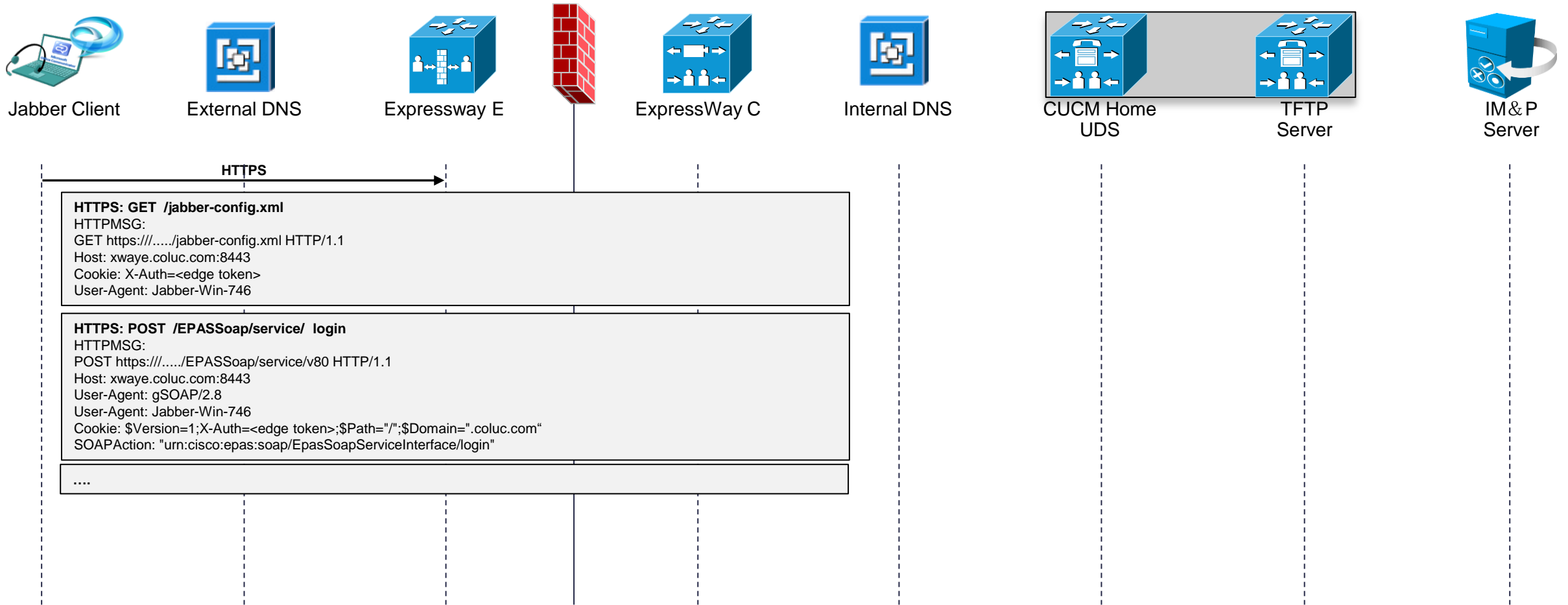
# Jabber Registration - Walk Trough

- Register Jabber client on UCM via MRA



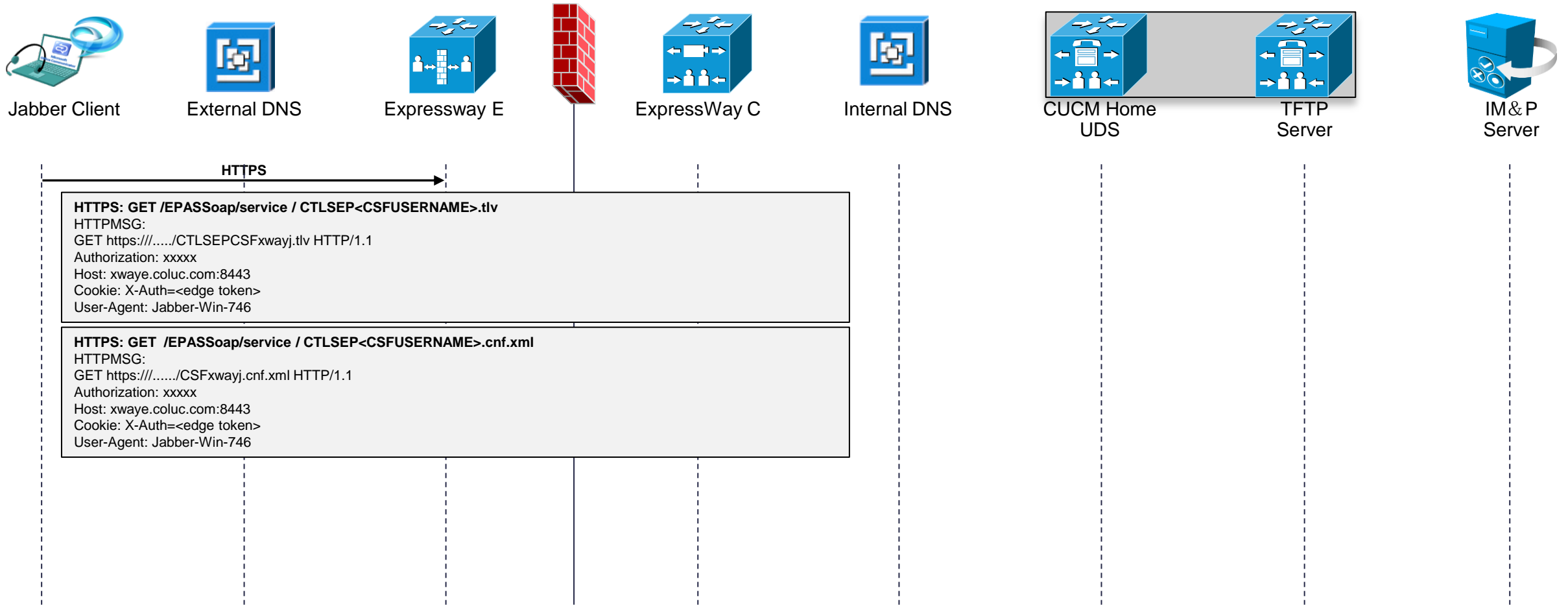
# Jabber Registration – Walk Through

- Register Jabber client on UCM via MRA



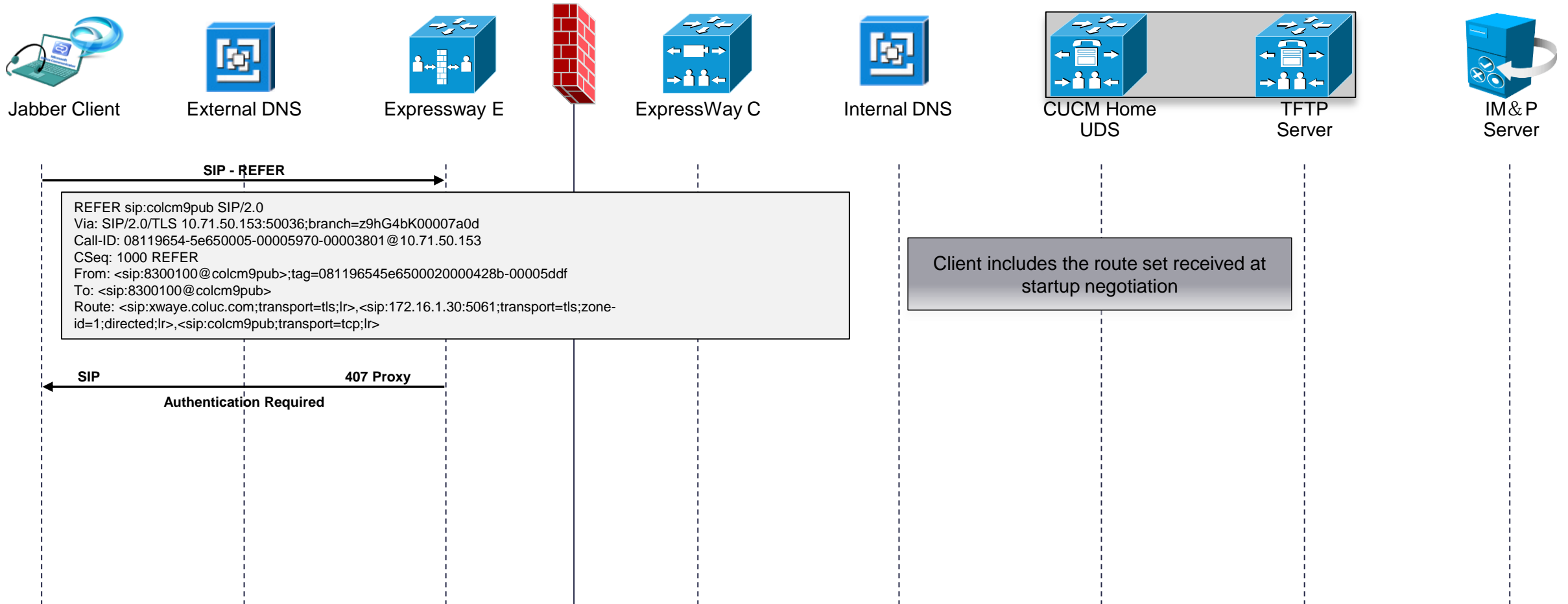
# Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



# Jabber Registration – Walk Through

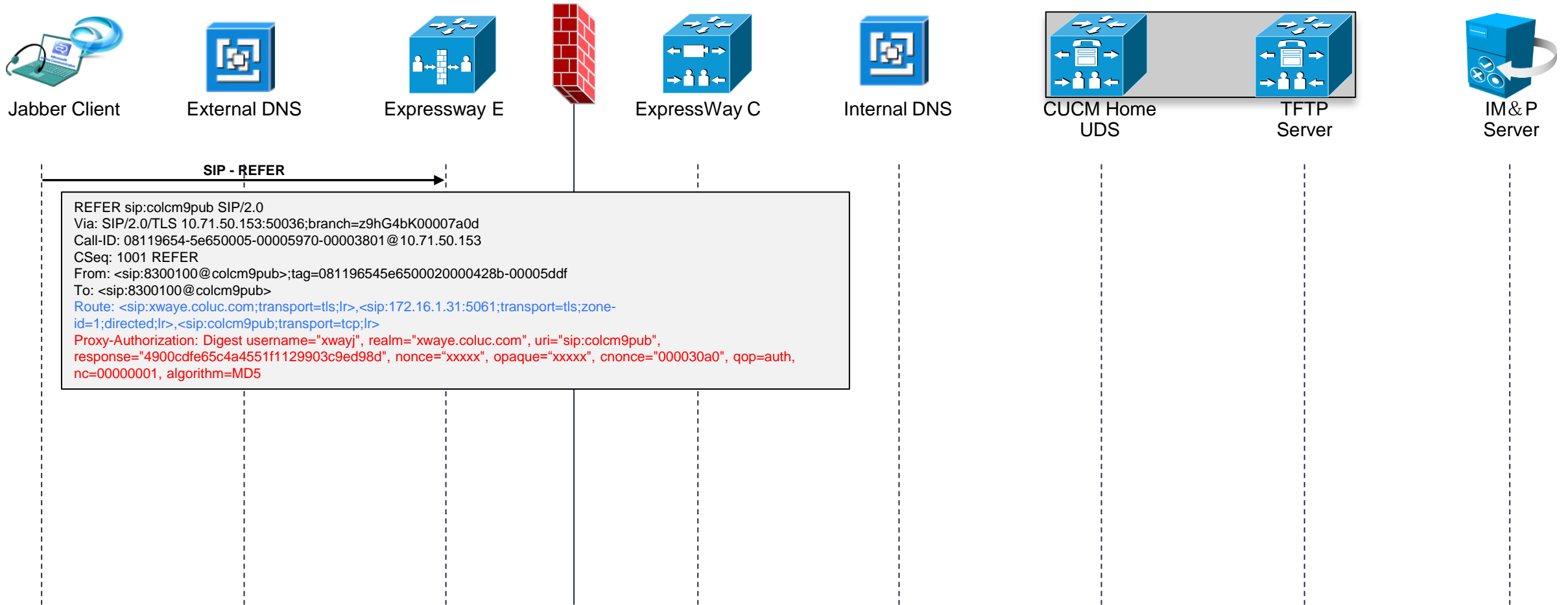
- Register Jabber client on UCM via MRA





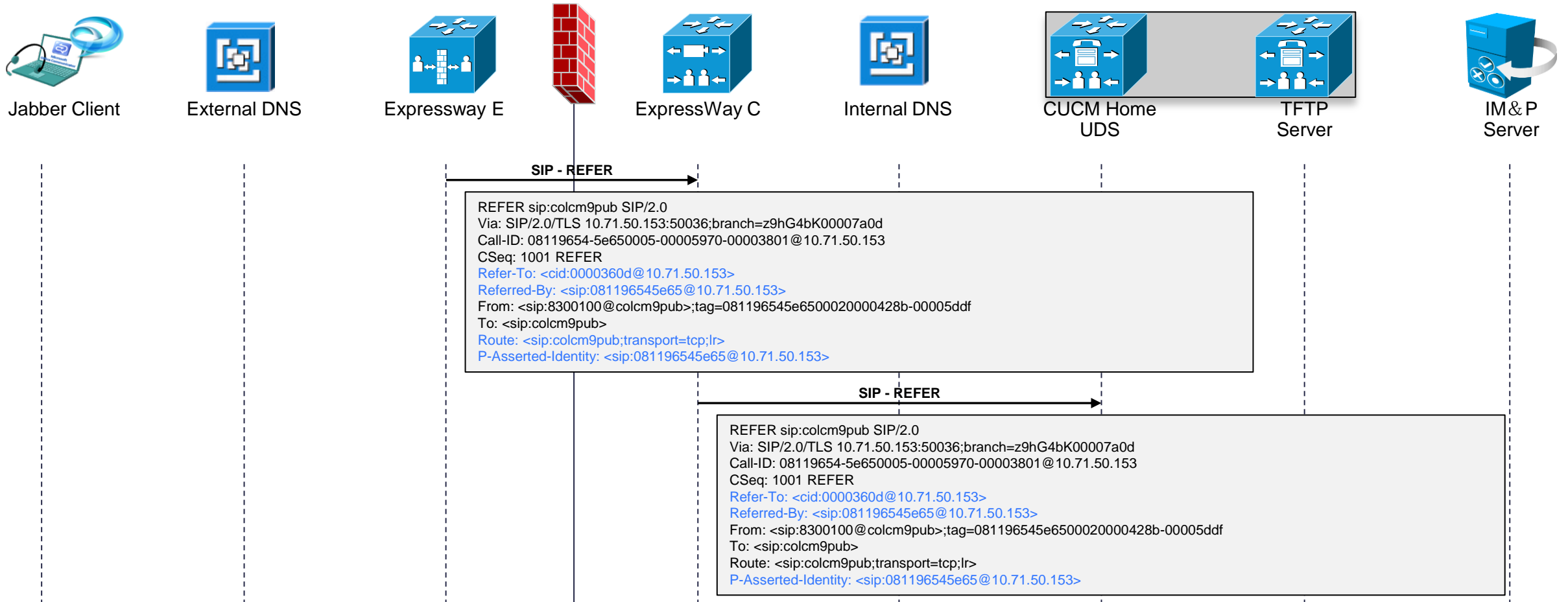
# Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



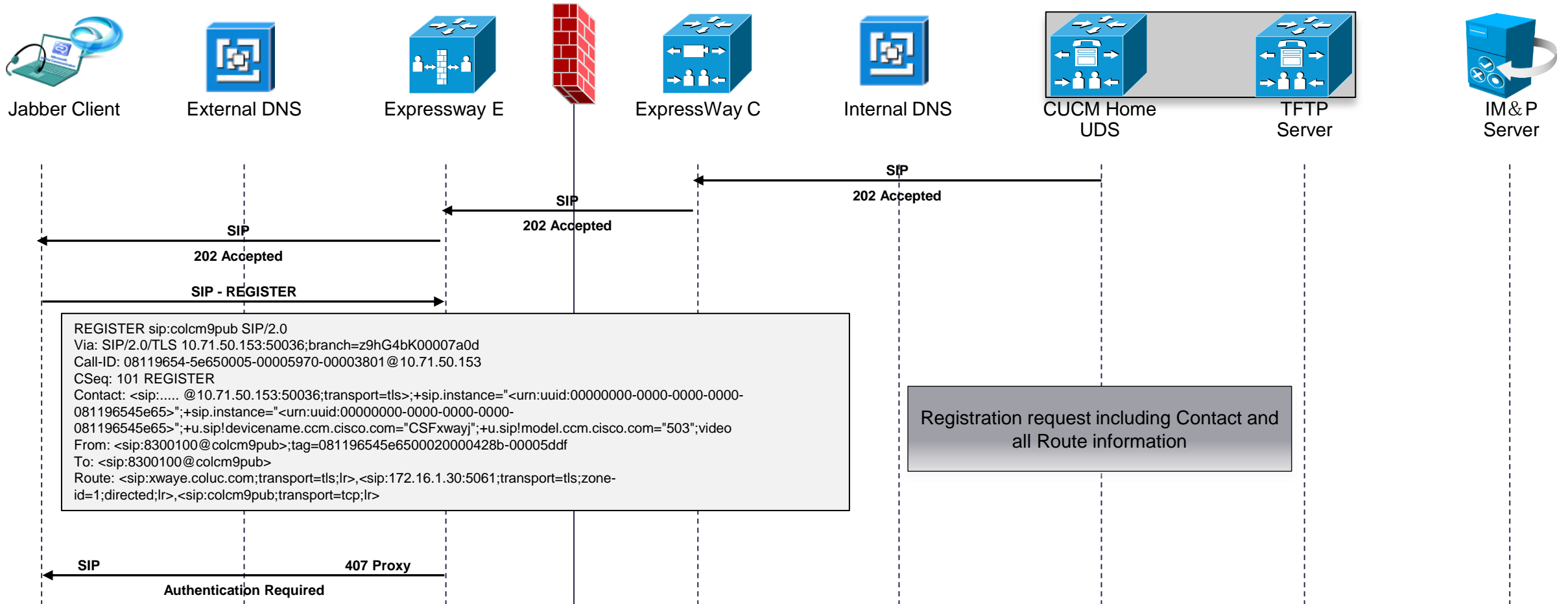
# Jabber Registration - Walk Through

- Register Jabber client on UCM via MRA



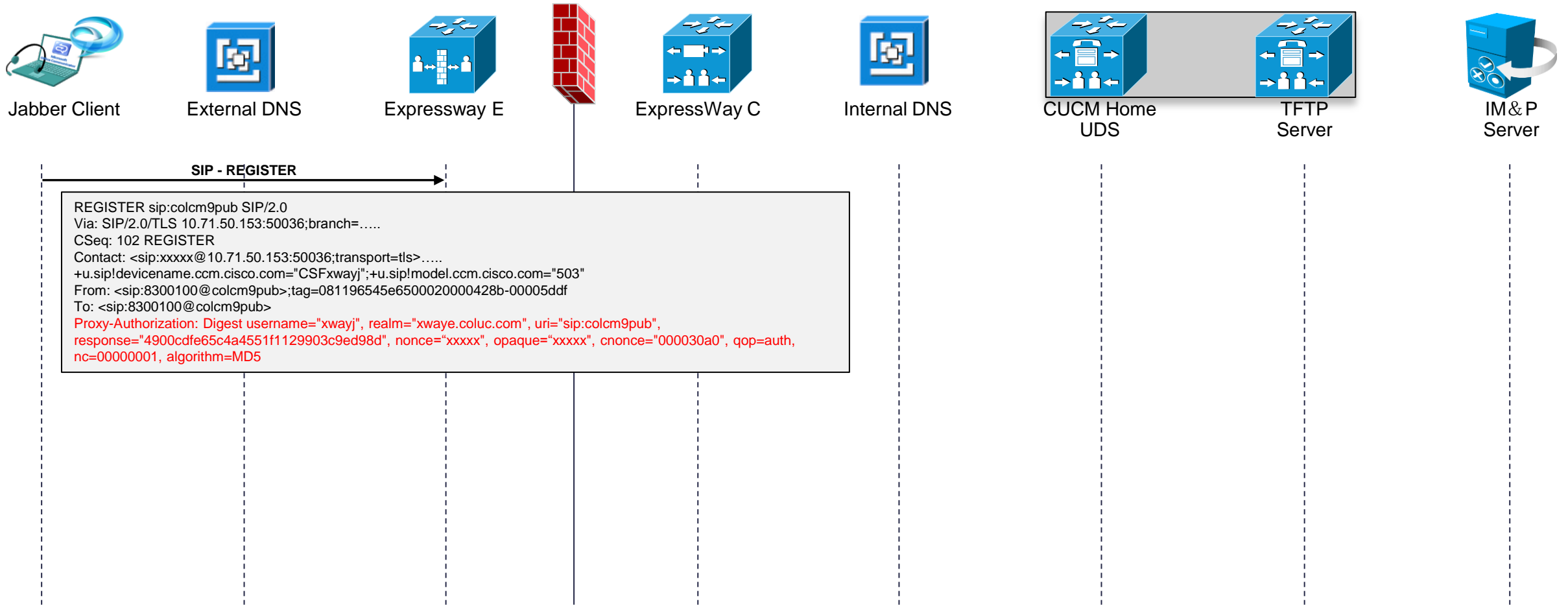
# Jabber Registration – Walk Through

- Register Jabber client on UCM via MRA



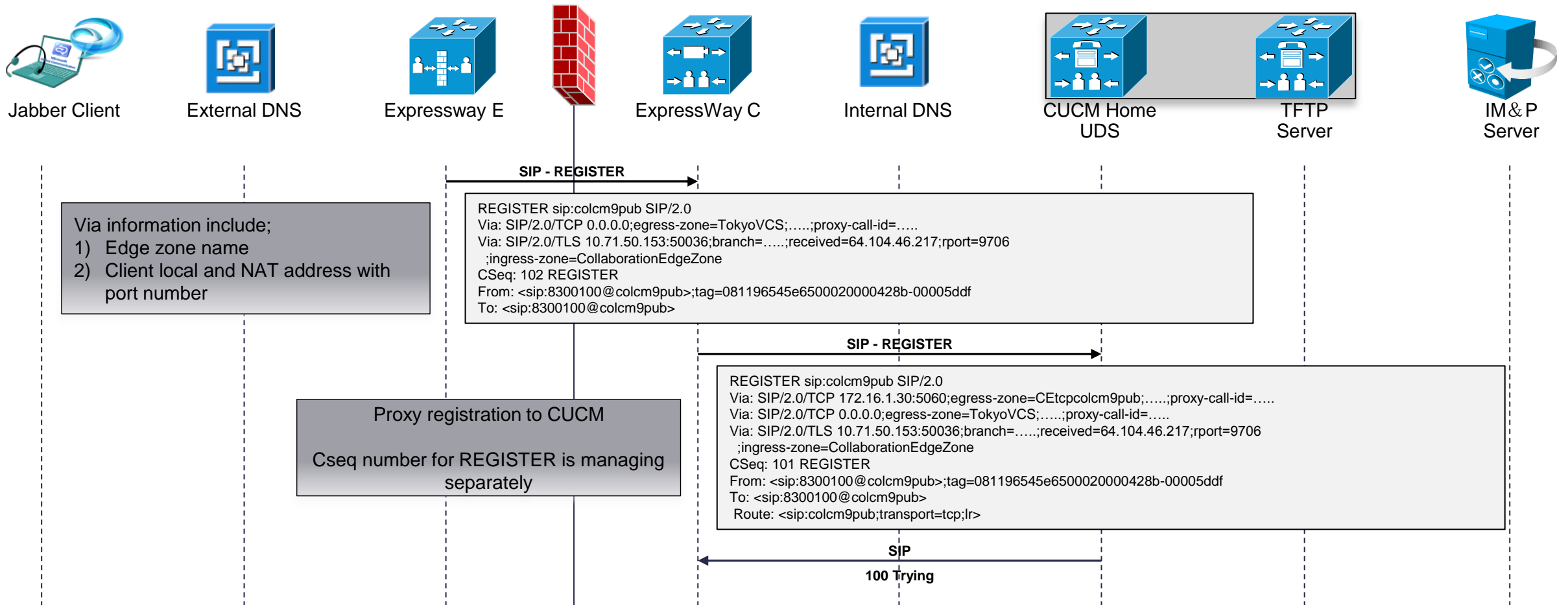
# Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



# Jabber Registration – Walk Through

- Register Jabber client on UCM via MRA



# References

# References

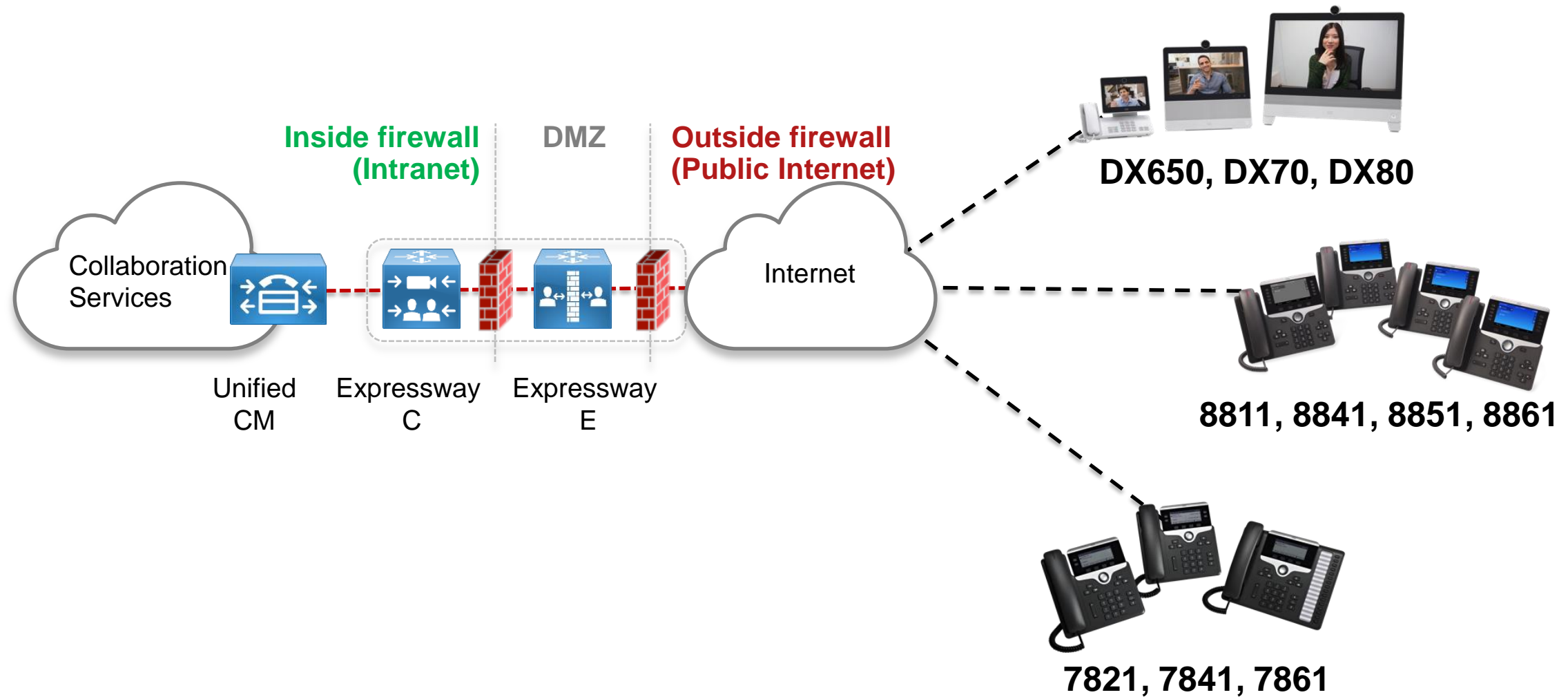
- X8.1.1 Mobile and Remote Access deployment guide  
<to be released soon>
- Jabber for Windows 9.7 install/config guide.  
(check chapter on deployment options for more on service discovery)  
[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/Windows/9\\_7/JAB\\_W\\_BK\\_C4C679C9\\_00\\_cisco-jabber-for-windows-97.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/9_7/JAB_W_BK_C4C679C9_00_cisco-jabber-for-windows-97.html)
- Jabber for Windows 9.7 release notes  
Doublecheck what is supported and what not when in edge mode  
[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/Windows/9\\_7/JAB\\_W\\_BK\\_CF8F083D\\_00\\_cisco-jabber-for-windows-97.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/9_7/JAB_W_BK_CF8F083D_00_cisco-jabber-for-windows-97.html)

# References

- Base64 encode/decode  
<http://www.base64decode.org/>



# New Endpoint Support



Thank you.

